PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-244419
(43)Date of publication of application : 29.08.2003

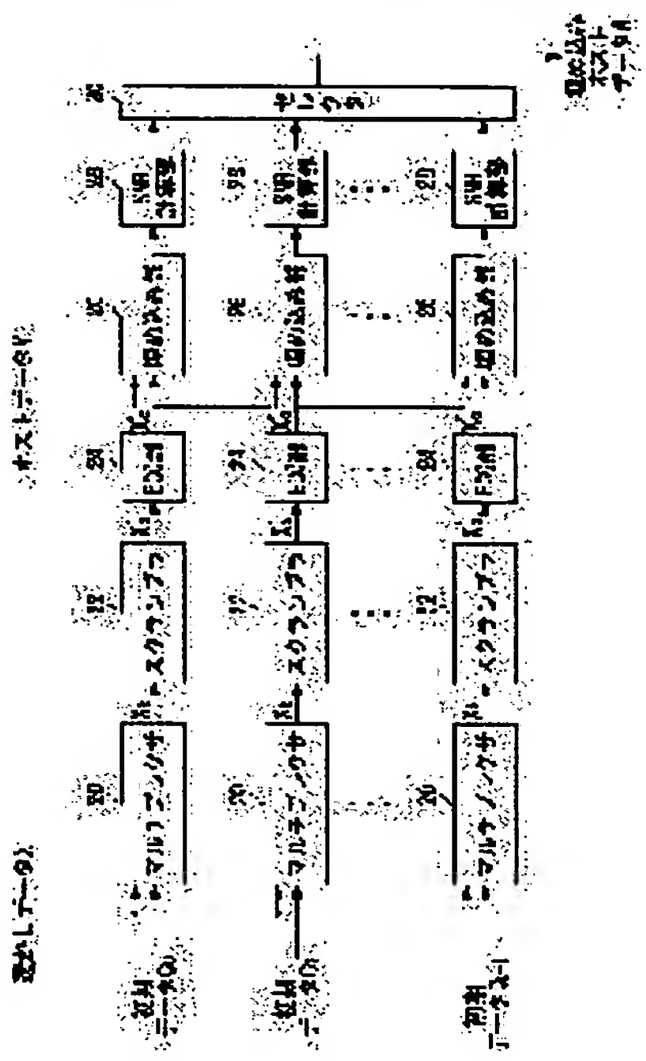
(51)Int.Cl. H04N 1/387
G06T 1/00
H04N 7/08
H04N 7/081

(21)Application number : 2002-036074
(22)Date of filing : 13.02.2002

(71)Applicant : SANYO ELECTRIC CO LTD
(72)Inventor : KUNIHAZAMA AKIOMI

(54) ELECTRONIC WATERMARK EMBEDDING METHOD, ENCODER AND DECODER CAPABLE OF UTILIZING SUCH METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To solve a problem that it is necessary to strengthen the durability of an electronic watermark since various kinds of operation are applied to the contents data embedded with an electronic watermark.
SOLUTION: A multiplexer 20 produces L kinds of bit sequences by inserting different initial data to the head of watermark data X. A scrambler 22 respectively scrambles the L kinds of bit sequences and produces L kinds of scrambled watermark data X' and an ECC part 24 adds a parity for an error correction to each of data. An embedding part 26 embeds the L kinds of scrambled watermark data X' into host data V and an SNR calculation part 28 evaluates the durability of the watermark data X concerning each of the host data V embedded with the watermark. A selector 30 selects the data of the strongest durability and outputs them as final embedded host data W.



LEGAL STATUS

[Date of request for examination] 24.10.2002
[Date of sending the examiner's decision of rejection] 06.09.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection] 2005-19447
[Date of requesting appeal against examiner's decision of rejection] 06.10.2005
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－244419
(P2003－244419A)
(43)公開日　平成15年８月29日(2003.8.29)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｈ０４Ｎ	1/387		Ｈ０４Ｎ 1/387		５Ｂ０５７
Ｇ０６Ｔ	1/00	５００	Ｇ０６Ｔ 1/00	５００Ｂ	５Ｃ０６３
Ｈ０４Ｎ	7/08		Ｈ０４Ｎ 7/08	Ｚ	５Ｃ０７６
	7/081				

審査請求　有　　請求項の数23　ＯＬ　（全 17 頁）

(21)出願番号　特願2002－36074(P2002－36074)

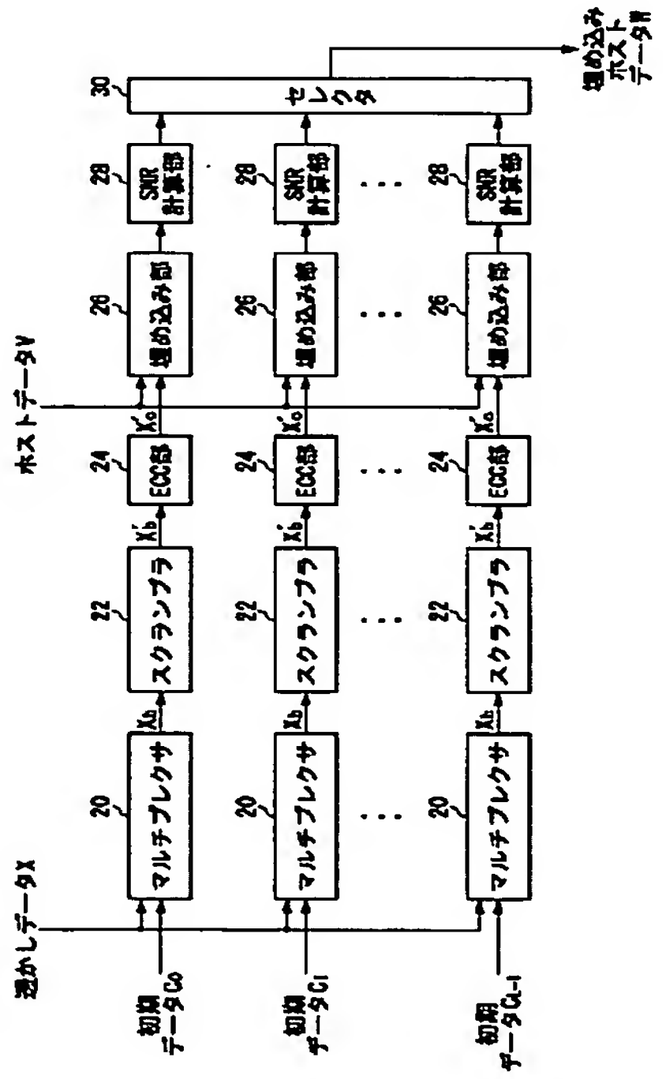
(22)出願日　平成14年２月13日(2002.2.13)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　国狭　亜輝臣
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100105924
弁理士　森下　賢樹

Ｆターム(参考)　5B057 CB19 CE08 CE09 CG07
5C063 AB03 AB07 AC01 AC05 CA11
CA23 DA07 DA13 DB09
5C076 AA14 BA06

(54)【発明の名称】　電子透かし埋め込み方法およびその方法を利用可能な符号化装置と復号装置

(57)【要約】
【課題】　電子透かしが埋め込まれたコンテンツデータにはさまざまな操作が加えられるため、電子透かしの耐性を強化しなければならない。
【解決手段】　マルチプレクサ２０は、透かしデータＸの先頭に異なる初期データを挿入してＬ種類のビット系列を生成する。スクランブラ２２はそのＬ種類のビット系列をそれぞれスクランブルして、Ｌ種類のスクランブルされた透かしデータＸ’を生成し、ＥＣＣ部２４はそれぞれに誤り訂正のためのパリティを付加する。埋め込み部２６は、Ｌ種類のスクランブルされた透かしデータＸ’のそれぞれをホストデータＶに埋め込み、ＳＮＲ計算部２８は、透かしの埋め込まれたホストデータＶのそれぞれについて、透かしデータＸの耐性を評価する。セレクタ３０は、耐性の最も強いものを選択し、最終的な埋め込みホストデータＷとして出力する。



【特許請求の範囲】

【請求項１】　ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成し、それらの透かしデータの候補がそれぞれ前記ホストデータに埋め込まれた場合における当該電子透かしの耐性を評価し、その評価が良好である前記透かしデータの埋め込みホストデータを取得することを特徴とする電子透かし埋め込み方法。

【請求項２】　電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成し、それらの埋め込み位置の候補のそれぞれに前記透かしデータが埋め込まれた場合における当該電子透かしの耐性を評価し、その評価が良好である前記埋め込み位置に前記透かしデータが埋め込まれた前記ホストデータを取得することを特徴とする電子透かし埋め込み方法。

【請求項３】　ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成するスクランブル部と、
前記複数の透かしデータの候補をそれぞれ前記ホストデータに埋め込み、複数の埋め込みホストデータの候補を生成する埋め込み部と、
前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する評価部と、
前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択して出力する選択部とを含むことを特徴とする符号化装置。

【請求項４】　電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、
前記ホストデータの前記複数の埋め込み位置の候補のそれぞれに前記透かしデータを埋め込み、複数の埋め込みホストデータの候補を生成する埋め込み部と、
前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する評価部と、
前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択して出力する選択部とを含むことを特徴とする符号化装置。

【請求項５】　前記評価部は、前記耐性を、前記ホストデータを前記透かしデータに対するノイズと見なした場合に計算されるＳＮ比により評価することを特徴とする請求項３または４に記載の符号化装置。

【請求項６】　前記評価部は、実際に埋め込まれた前記透かしデータと硬判定に基づいて抽出される透かしデータとを比較することにより、前記耐性を評価することを特徴とする請求項３または４に記載の符号化装置。

【請求項７】　前記評価部は、前記埋め込みホストデータに対して有用性のある操作を施した上で、前記耐性を評価することを特徴とする請求項３から６のいずれかに記載の符号化装置。

【請求項８】　前記評価部は、前記埋め込みホストデータを圧縮符号化する際の量子化誤差を考慮して前記耐性を評価することを特徴とする請求項３から６のいずれかに記載の符号化装置。

【請求項９】　前記スクランブル部は、スクランブルにより生成される前記透かしデータの候補のデータの一部に、スクランブルを解除するために必要な識別データを含めることを特徴とする請求項３に記載の符号化装置。

【請求項１０】　前記スクランブル部によるスクランブルの後、スクランブルを解除するために必要な識別データが秘密鍵として保持されることを特徴とする請求項３に記載の符号化装置。

【請求項１１】　前記スクランブル部は、前記識別データに基づく演算により、前記電子透かしデータをスクランブルすることを特徴とする請求項９または１０に記載の符号化装置。

【請求項１２】　前記識別データは前記透かしデータの候補を識別する情報であり、前記スクランブル部は、前記識別データを用いて前記電子透かしデータに畳み込み演算を施すことにより、前記電子透かしデータをスクランブルすることを特徴とする請求項９または１０に記載の符号化装置。

【請求項１３】　前記位置情報生成部は、前記埋め込み位置の候補を識別するための識別データとランダムな埋め込み位置とを対応づけたテーブルを参照することにより、前記複数の埋め込み位置の候補を生成することを特徴とする請求項４に記載の符号化装置。

【請求項１４】　前記位置情報生成部による埋め込み位置の候補の生成後、前記識別データが秘密鍵として保持されることを特徴とする請求項１３に記載の符号化装置。

【請求項１５】　電子透かしの埋め込まれたホストデータからスクランブルされた透かしデータを抽出する抽出部と、
前記スクランブルされた透かしデータの識別データをもとに、前記透かしデータに畳み込み演算を施すことにより、前記透かしデータのスクランブルを解除するデスクランブル部とを含むことを特徴とする復号装置。

【請求項１６】　前記デスクランブル部は、前記識別データを前記スクランブルされた透かしデータの一部から取得することを特徴とする請求項１５に記載の復号装置。

【請求項１７】　前記デスクランブル部は、前記識別データを秘密鍵として取得することを特徴とする請求項１５に記載の復号装置。

【請求項１８】　電子透かしが埋め込まれたホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、
前記複数の埋め込み位置の候補のそれぞれを用いて前記ホストデータに埋め込まれた透かしデータの候補を複数抽出する抽出部と、

前記抽出された複数の透かしデータの候補を想定される透かしデータとの間で照合する照合部と、
前記照合部による照合結果に基づいて前記複数の透かしデータの候補の一つを選択して出力する選択部とを含むことを特徴とする復号装置。
【請求項１９】　前記位置情報生成部は、前記埋め込み位置の候補を識別するための識別データとランダムな埋め込み位置とを対応づけたテーブルを参照することにより、前記複数の埋め込み位置の候補を生成することを特徴とする請求項１８に記載の復号装置。
【請求項２０】　電子透かしが埋め込まれたホストデータの埋め込み位置を識別するための識別データを秘密鍵として取得し、前記秘密鍵に基づいて、前記埋め込み位置の候補を識別するための識別データとランダムな埋め込み位置とを対応づけたテーブルを参照することにより、前記埋め込み位置を特定する位置情報生成部と、
前記特定された埋め込み位置を用いて前記ホストデータに埋め込まれた透かしデータを抽出する抽出部とを含むことを特徴とする復号装置。
【請求項２１】　電子透かしデータが埋め込まれたホストデータの構造であって、
前記ホストデータに埋め込まれるべき電子透かしデータが所定のスクランブル方式によりスクランブルされた形態で前記ホストデータに埋め込まれており、そのスクランブルされた透かしデータの一部にスクランブルを解除するために必要な当該透かしデータの識別データが含まれることを特徴とするコンピュータにて読み取りおよび利用が可能なデータ構造。
【請求項２２】　ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成する工程と、
前記複数の透かしデータの候補をそれぞれ前記ホストデータに埋め込み、複数の埋め込みホストデータの候補を生成する工程と、
前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する工程と、
前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択する工程とをコンピュータに実行させることを特徴とするコンピュータプログラム。
【請求項２３】　電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成する工程と、
前記ホストデータの前記複数の埋め込み位置の候補のそれぞれに前記透かしデータを埋め込み、複数の埋め込みホストデータの候補を生成する工程と、
前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する工程と、
前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択する工程とをコンピュータに実行させることを特徴とするコンピュータプログラム。
【発明の詳細な説明】

【０００１】
【発明の属する技術分野】この発明は、電子透かし技術に関し、特に電子透かしの埋め込み方法、およびその方法を利用可能な符号化装置と復号装置に関する。
【０００２】
【従来の技術】ここ数年、インターネット利用人口が急増し、インターネット利用の新たなステージともいえるブロードバンド時代に入ろうとしている。ブロードバンド通信では通信帯域が格段に広がるため、音声、静止画、動画などデータ量の大きいコンテンツの配信も気軽にできるようになる。このようなデジタルコンテンツの流通が盛んになると、コンテンツの著作権の保護がより一層求められることになる。
【０００３】ネットワーク上に流通するコンテンツのデータは他人に容易にコピーされ、著作権に対する保護が十分ではないのが現状である。そこで著作権を保護するために、コンテンツの作成者や利用者の情報を電子透かしとしてコンテンツデータに埋め込む技術が開発されている。この電子透かし技術を用いることにより、ネットワーク上で流通するコンテンツデータから電子透かしを抽出して、不正利用を検出したり、不正コピーの流通経路を追跡することが可能となる。
【０００４】
【発明が解決しようとする課題】電子透かしは、不正利用者による改ざんを防止するために、利用者には分からないようにコンテンツデータに埋め込まれる。しかしコンテンツデータは、流通過程や利用過程で、圧縮符号化や各種フィルタリングなどの信号処理が加えられたり、ユーザにより加工されたり、あるいは透かし情報が改ざんされるなど、さまざまな操作を受けることがあり、その過程で埋め込まれた電子透かしデータの一部が変更されたり、消失する可能性がある。したがって電子透かしはこういった操作に対する耐性が要求される。
【０００５】電子透かしの耐性を高めるためにさまざまな電子透かしの埋め込み技術が開発されている。たとえば、特開２０００－１３５８７号公報は、電子透かし情報を埋め込む処理の自由度を維持しつつ、耐性の強い電子透かしの埋め込みを可能とする埋め込み方法が開示されている。このような電子透かし技術は、人間の視覚特性に合わせて、画像のエッジ部分やテクスチャ領域の中でも変化の大きな部分など高周波成分に電子透かしを埋め込む方法であり、個々のコンテンツデータの内容に強く依存し、透かし埋め込み後のコンテンツデータに対するさまざまな操作に対して耐性を強化するには、汎用性や柔軟性の面で限界がある。
【０００６】本発明はこうした状況に鑑みてなされたもので、その目的は、耐性の強い電子透かしを埋め込み、電子透かしの検出誤差を低減することの可能な技術の提供にある。
【０００７】

【課題を解決するための手段】本発明のある態様は電子透かし埋め込み方法に関する。この方法は、ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成し、それらの透かしデータの候補がそれぞれ前記ホストデータに埋め込まれた場合における当該電子透かしの耐性を評価し、その評価が良好である前記透かしデータの埋め込みホストデータを取得する。この方法によれば、ホストデータに応じて、透かしデータを耐性の強いデータ系列に変換した後に埋め込むことができ、電子透かしの検出誤差を低減することができる。

【０００８】ホストデータは、電子透かしを埋め込む対象となるオリジナルデータであり、たとえば静止画、動画、音声などのデータである。埋め込まれる電子透かしには、オリジナルデータの識別情報、作成者情報、利用者情報などが含まれる。その他、認証を目的として、ホストデータのダイジェストデータ、すなわちホストデータの特徴を端的に表したデータを電子透かしとして埋め込むことも可能である。電子透かしの耐性とは、電子透かしの埋め込まれたホストデータが改変されるなどの攻撃を受けた場合や、埋め込みホストデータに圧縮符号化やフィルタリングなどの信号処理が施された場合など、埋め込みホストデータに対して何らかの操作が加えられた場合に電子透かしデータがもつ頑強性をいう。

【０００９】電子透かしを埋め込む側では、電子透かしデータをスクランブルする際、元の電子透かしデータを複数の透かしデータの候補に対応づける１対多の写像が用いられる。電子透かしを抽出する側では、逆写像を行って、スクランブルされた透かしデータから元の電子透かしデータを得る。そのため電子透かしを抽出する側では、元の電子透かしデータと複数の透かしデータの候補の対応テーブルが利用されてもよい。また、電子透かしを埋め込む側で、元の電子透かしデータから所定の初期値のもとで複数の透かしデータの候補を生成するスクランブル関数が利用されてもよい。この場合、電子透かしを抽出する側では、スクランブルに利用された初期値とスクランブル関数にもとづいて、抽出された電子透かしの逆スクランブルが行われる。

【００１０】本発明の別の態様も電子透かし埋め込み方法に関する。この方法は、電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成し、それらの埋め込み位置の候補のそれぞれに前記透かしデータが埋め込まれた場合における当該電子透かしの耐性を評価し、その評価が良好である前記埋め込み位置に前記透かしデータが埋め込まれた前記ホストデータを取得する。埋め込み位置の候補は、初期埋め込み位置を所定の初期値のもとでスクランブル関数によりスクランブルすることで生成してもよい。この方法によれば、ホストデータの応じて、耐性が強い埋め込み位置を検出して、電子透かしを埋め込むことができる。

【００１１】本発明のさらに別の態様は符号化装置に関する。この装置は、ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成するスクランブル部と、前記複数の透かしデータの候補をそれぞれ前記ホストデータに埋め込み、複数の埋め込みホストデータの候補を生成する埋め込み部と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する評価部と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択して出力する選択部とを含む。

【００１２】本発明のさらに別の態様も符号化装置に関する。この装置は、電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、前記ホストデータの前記複数の埋め込み位置の候補のそれぞれに前記透かしデータを埋め込み、複数の埋め込みホストデータの候補を生成する埋め込み部と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する評価部と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択して出力する選択部とを含む。

【００１３】前記スクランブル部は、前記識別データに基づく演算により、前記電子透かしデータをスクランブルしてもよい。この演算はスクランブル多項式その他の変換式により透かしデータを変換する演算であってもよい。前記スクランブル部は、前記透かしデータの候補を識別するための識別データを用いて前記電子透かしデータに畳み込み演算を施すことにより、前記電子透かしデータをスクランブルしてもよい。この畳み込み演算により、多様性に富んだ透かしデータの候補を生成することができる。埋め込み位置の候補を生成する際にも、このスクランブル方式が用いられてもよい。また埋め込み位置の候補を識別するための識別データとランダムな埋め込み位置とを対応づけたテーブルを参照することにより、複数の埋め込み位置の候補を生成してもよい。

【００１４】前記スクランブル部は、スクランブルにより生成される前記透かしデータの候補のデータの一部に、スクランブルを解除するために必要な識別データを含めてもよい。前記スクランブル部によるスクランブルの後、スクランブルを解除するために必要な識別データが秘密鍵として保持されてもよい。この識別データはスクランブル方式を特定する情報、たとえばスクランブルの種類、スクランブルの変換式または逆変換式を識別する情報であってもよい。またこの識別データはスクランブルを解除するために必要な初期データを含んでもよい。復号側でスクランブルされた電子透かしを抽出した際、この識別データをもとにしてスクランブルを解除して、元の電子透かしデータを得ることができる。

【００１５】上記のいずれの符号化装置においても、前記評価部は、前記耐性を、前記ホストデータを前記透かしデータに対するノイズと見なした場合に計算されるＳ

Ｎ比により評価してもよい。特にターボ符号化などの軟入力誤り訂正符号の場合には、ＳＮ比に基づいた評価基準で候補を選択することにより、ビット誤り率（ＢＥＲ）を低減することができる。また、前記評価部は、実際に埋め込まれた前記透かしデータと硬判定に基づいて抽出される透かしデータとを比較することにより、前記耐性を評価してもよい。この比較のために、硬判定により抽出される透かしデータと実際に埋め込まれた透かしデータとの間のハミング距離もしくはユークリッド距離を評価してもよい。この場合、距離が大きいほど、誤差が大きいため、強度は低いと判断される。この評価基準により、正しく硬判定復号されるビット数が最も多い透かしデータの候補が選択される。特に硬入力に基づいた誤り訂正符号を用いる場合は、このような硬判定結果との比較評価基準で候補を選択することにより、ビット誤り率を低く抑えることができる。

【００１６】前記評価部は、前記埋め込みホストデータに対して有用性のある操作を施した上で、前記耐性を評価してもよい。有用性のある操作とは、たとえば圧縮符号化や各種フィルタリングなどの信号処理、スケーリングや回転などの幾何学的変換などである。前記評価部は、前記埋め込みホストデータを圧縮符号化する際の量子化誤差を考慮して前記耐性を評価してもよい。前記耐性をＳＮ比で評価する場合、埋め込みホストデータに有用性のある操作を施した後に抽出される透かしデータと実際に埋め込まれた透かしデータとの間の分散を評価してもよい。

【００１７】本発明のさらに別の態様は復号装置に関する。この装置は、電子透かしの埋め込まれたホストデータからスクランブルされた透かしデータを抽出する抽出部と、前記スクランブルされた透かしデータの識別データをもとに、前記透かしデータに畳み込み演算を施すことにより、前記透かしデータのスクランブルを解除するデスクランブル部とを含む。前記デスクランブル部は、前記識別データを前記スクランブルされた透かしデータの一部から取得してもよい。

【００１８】本発明のさらに別の態様も復号装置に関する。この装置は、電子透かしが埋め込まれるホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、前記複数の埋め込み位置の候補のそれぞれを用いて前記ホストデータに埋め込まれた透かしデータの候補を複数抽出する抽出部と、前記抽出された複数の透かしデータの候補を、想定される透かしデータとの間で照合する照合部と、前記照合部による照合結果に基づいて前記複数の透かしデータの候補の一つを選択して出力する選択部とを含む。

【００１９】本発明のさらに別の態様はコンピュータにて読み取りおよび利用が可能なデータ構造に関する。このデータ構造は、電子透かしデータが埋め込まれたホストデータの構造であり、ホストデータに埋め込まれるべき電子透かしデータが所定のスクランブル方式によりスクランブルされた形態で前記ホストデータに埋め込まれており、そのスクランブルされた透かしデータの一部にスクランブルを解除するために必要な当該透かしデータの識別データが含まれる。

【００２０】本発明のさらに別の態様はコンピュータプログラムに関する。このプログラムは、ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成する工程と、前記複数の透かしデータの候補をそれぞれ前記ホストデータに埋め込み、複数の埋め込みホストデータの候補を生成する工程と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する工程と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択する工程とをコンピュータに実行させる。

【００２１】本発明のさらに別の態様もコンピュータプログラムに関する。このプログラムは、電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成する工程と、前記ホストデータの前記複数の埋め込み位置の候補のそれぞれに前記透かしデータを埋め込み、複数の埋め込みホストデータの候補を生成する工程と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する工程と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択する工程とをコンピュータに実行させる。

【００２２】なお、以上の構成要素の任意の組み合わせ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【００２３】

【発明の実施の形態】実施の形態１

図１は、実施の形態１に係る符号化装置１０の構成を示す。この構成は、ハードウエア的には、任意のコンピュータのＣＰＵ、メモリ、その他のＬＳＩで実現でき、ソフトウエア的にはメモリにロードされた電子透かし埋め込み機能のあるプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックがハードウエアのみ、ソフトウエアのみ、またはそれらの組み合わせによっていろいろな形で実現できることは、当業者には理解されるところである。

【００２４】符号化装置１０は、ホストデータＶに透かし情報Ｉを埋め込む処理を行い、埋め込みホストデータＷを出力する。ホストデータＶは、たとえば音声、静止画、動画などのデータである。透かし情報Ｉは、そのホストデータＶの識別情報、作成者情報、利用者情報など著作権に関する情報、ホストデータＶの改ざん検出を行う認証情報、タイムスタンプなどである。

【００２５】暗号化部１２は、ホストデータＶに埋め込むべき透かし情報Ｉを秘密鍵Ｋにより暗号化し、透かしデータＸを出力する。暗号化の関数をf_0とすると、この処理は変換式Ｘ＝f_0（Ｉ，Ｋ）で表される。透かし情報の暗号化を行わない場合には、暗号化部１２の構成は省略してもよい。

【００２６】変更部１４は、透かしデータＸとホストデータＶを用いて、透かしデータＸをスクランブルし、スクランブルされた透かしデータＸ’を出力する。スクランブルの関数をf_2とすると、この処理は変換式Ｘ’＝f_2（Ｘ，Ｖ）で表される。

【００２７】埋め込み部１６は、秘密鍵Ｋを用いて、スクランブルされた透かしデータＸ’をホストデータＶに埋め込み、埋め込みホストデータＷを出力する。埋め込みの関数をf_1とすると、この処理は変換式Ｗ＝f_1（Ｖ，Ｘ’，Ｋ）で表される。秘密鍵Ｋに依存しない埋め込み方式の場合は、Ｗ＝f_1（Ｖ，Ｘ’）となる。

【００２８】変更部１４と埋め込み部１６は協同して、複数のスクランブルされた透かしデータＸ’を生成し、それぞれをホストデータＶに埋め込み、複数の埋め込みホストデータＷの候補を生成し、それらの候補の一つを選択する機能をもつ。

【００２９】図２は変更部１４と埋め込み部１６の機能構成図である。Ｌ個のマルチプレクサ２０は、透かしデータＸの先頭にそれぞれ初期データC_0～C_{L-1}を挿入したＬ種類のビット系列X_bを生成する。Ｌ個のスクランブラ２２はＬ種類のビット系列をそれぞれスクランブルして、Ｌ種類のスクランブルされた透かしデータX'_bを生成する。Ｌ個のＥＣＣ（Error Correction Code）部２４はＬ種類のスクランブルされた透かしデータX'_bのそれぞれに誤り訂正のためのパリティを付加した透かしデータX'_cを生成する。ＥＣＣ部２４は、透かしビットの検出率を向上させるためのオプションであって、アプリケーションによっては必要ない場合もあり、この構成を省略してもよい。

【００３０】Ｌ個の埋め込み部２６は、Ｌ種類のスクランブルされた透かしデータX'_cのそれぞれをホストデータＶに埋め込み、Ｌ種類の埋め込みホストデータＷの候補を生成する。Ｌ個のＳＮＲ計算部２８は、Ｌ種類の埋め込みホストデータＷの候補のそれぞれについて、透かしデータＸの耐性を評価する。セレクタ３０は、耐性の評価値が最良である埋め込みホストデータＷの候補を選択し、それを最終的な埋め込みホストデータＷとして出力する。

【００３１】図３は、実施の形態１に係る復号装置４０の構成を示す。符号化装置１０により電子透かしが埋め込まれた埋め込みホストデータＷは、ネットワーク上で流通し、コンピュータにおいて利用される。その過程で埋め込みホストデータＷは圧縮符号化や改ざんなどの操作を受ける。画像データであれば、ＪＰＥＧ圧縮、フィルタリング、量子化、色補正などの信号処理や、スケーリング、クロッピング、回転、並行移動等の幾何学的な変換など有用性のある操作が施されたり、電子透かしを除去したり改変するなどの不正な攻撃が加えられたりする。そのような操作による変形を埋め込みホストデータＷに対するノイズＮとみなし、ノイズＮが付加した埋め込みホストデータＷを埋め込みホスト信号Ｗ’（＝Ｗ＋Ｎ）とする。復号装置４０は、埋め込みホスト信号Ｗ’から埋め込まれた透かしデータＸを抽出する処理を行う。

【００３２】抽出部４２は、秘密鍵Ｋを用いて、埋め込みホスト信号Ｗ’に埋め込まれた透かしデータX'_cを抽出する。ＥＣＣ復号部４４はこの透かしデータX'_cに付加されているパリティビットを用いて誤り訂正を行い、透かしデータX'_bを生成する。デスクランブラ４６は秘密鍵Ｋを用いて、誤り訂正後の透かしデータX'_bのスクランブルを解除し、透かしデータX_bを出力する。図示しないが、この透かしデータX_bはさらに、秘密鍵Ｋにより復号されて元の透かし情報Ｉが得られる。

【００３３】以上の構成の符号化装置１０および復号装置４０による電子透かしの埋め込みと抽出の手順を説明する。図８は、符号化装置１０による電子透かしの埋め込み手順を説明するフローチャートである。フローチャートの説明にあたり、図４から図７を適宜参照する。マルチプレクサ２０は、暗号化部１２により暗号化された透かしデータＸの先頭にＬ種類の初期データを挿入してＬ個の符号系列を生成し（Ｓ１０）、スクランブラ２２は、それらの符号系列をスクランブルしてＬ種類のスクランブルされた透かしデータＸ’を生成する（Ｓ１２）。

【００３４】図４は、透かしデータＸとＬ種類のスクランブルされた透かしデータＸ’との関係を示す。ｎビットの透かしデータＸの先頭に、ｒビットの冗長語を識別データＩＤ［０］～ＩＤ［Ｌ－１］として付加し、Ｌ種類の透かしデータの候補を作成する。最大2^r種類の候補が作成される。これらの候補に含まれる透かしデータＸのビット列はこれから述べるスクランブル方式により、スクランブルされる。

【００３５】スクランブル方式の一例として、伝送や磁気記録におけるデジタル変調の際に利用されるＧＳ（Guided Scramble）方式を採用する。ＧＳ方式は、ある一定のデータブロック長からなる情報系列に対して、Ｌ種類の符号系列を生成し、これらを次に送信する符号系列の候補として扱う。これらの候補の中から、伝送媒体の性質に合わせて最適なものを選択して最終的な符号系列とする。このＧＳ方式により、多様性に富んだ符号系列の候補を簡単な方法で生成することができる。

【００３６】符号化装置１０におけるマルチプレクサ２０とスクランブラ２２がＧＳ符号化器として機能する。ＧＳ符号化器は、ｎビットからなる情報系列Ｄ（ｘ）の

11

直前にＬ種類のｒビットの冗長語ｃｉ（ｉ＝０，・・・，Ｌ－１）を付加し、Ｌ種類の符号系列ｃｉ ｘ^ｎ ＋Ｄ（ｘ）を生成する。この符号系列の符号長は（ｎ＋ｒ）ビットとなる。このようにして冗長語が付加された符号＊

$$T_i(x) = Q_{s(x)} \quad [(c_i x^n + D(x)) x^N] \qquad (1)$$

ただし、Ｑ．［ｂ］はｂをａで除算した商を示す。商集合｛Ｔ０（ｘ），・・・，ＴＬ－１　（ｘ）｝がスクランブル後の符号系列の候補である。これらの候補の各々について、その符号系列が実際に用いられた際の性能を評価し、その評価値が最良であるものを最終的な符号系列として選択する。

【００３８】復調時には、復号装置４０におけるデスクランブラ４６がＧＳ復号器として機能し、符号系列にＳ（ｘ）を乗算し、下位Ｎビットと上位ｒビットの変換情報を捨てることにより、元の情報系列Ｄ（ｘ）が得られる。

【００３９】ここでスクランブル多項式Ｓ（ｘ）として、Ｓ（ｘ）＝ｘ^ｒ ＋１を用いた場合を説明する。ｎ　ｍｏｄ　ｒ＝０の場合、（１）式は次式に示す畳み込み演算で表現可能である。

【００４０】$t_j = d_j$ （＋）c_i　（ｊ＝０）

$t_j = d_j$ （＋）t_{j-1}　（ｊ＝１，・・・，ｎ／ｒ－１）

ただし、ｉ＝０，・・・，Ｌ－１であり、d_j は元の情報系列Ｄ（ｘ）をｒビットずつ区切ったビット列、t_j は変換後の符号系列Ｔｉ（ｘ）の先頭のｒビットの冗長語ｃｉ以降をｒビットずつ区切ったビット列である。また（＋）は排他的論理和（ＥＸ－ＯＲ）演算を示す。

【００４１】図５はこの符号化時の畳み込み演算を説明する図である。たとえば、ｎ＝６、ｒ＝２の場合を考える。元の情報系列Ｄ（ｘ）＝（１，０，１，０，０，１）に対して、冗長語c_0＝（０，０）を付加して、変換後の符号系列Ｔ０（ｘ）を生成する。上記の符号化時の畳み込み演算により、$t_0 = d_0$ （＋）c_0 ＝（１，０）（＋）（０，０）＝（１，０）、$t_1 = d_1$ （＋）t_0 ＝（１，０）（＋）（１，０）＝（０，０）、$t_2 = d_2$ （＋）t_1 ＝（０，１）（＋）（０，０）＝（０，１）となり、変換後の符号系列T_0＝（０，０，１，０，０，０，０，１）が得られる。ここで変換後の符号系列Ｔ０の先頭の２ビットは冗長語c_0であることに注意する。

※【００４２】同様にして、冗長語c_1＝（０，１）、c_2＝（１，０）、c_3＝（１，１）に対して、それぞれ変換後の符号系列T_1＝（０，１，１，１，０，１，０，０）、T_2＝（１，０，０，０，１，０，１，１）、T_3＝（１，１，０，１，１，１，１，０）が得られる。

【００４３】復号時は次式のように畳み込み演算を行うことにより、元の情報系列Ｄ（ｘ）が得られる。

【００４４】$d_j = t_j$ （＋）c_i　（ｊ＝０）

$d_j = t_j$ （＋）t_{j-1}　（ｊ＝１，・・・，ｎ／ｒ－１）

【００４５】図６はこの復号時の畳み込み演算を説明する図である。前述の例において、変換後の符号化系列T_0＝（０，０，１，０，０，０，０，１）が与えられると、先頭の２ビットから冗長語c_0＝（０，０）が得られ、上記の復号時の畳み込み演算により、$d_0 = t_0$ （＋）c_0 ＝（１，０）（＋）（０，０）＝（１，０）、$d_1 = t_1$ （＋）t_0 ＝（０，０）（＋）（１，０）＝（１，０）、$d_2 = t_2$ （＋）t_1 ＝（０，１）（＋）（０，０）＝（０，１）となり、元の情報系列Ｄ（ｘ）＝（１，０，１，０，０，１）が得られる。他の変換後の符号化系列T_1，T_2，T_3についてもこの畳み込み演算により、元の情報系列Ｄ（ｘ）が得られる。

【００４６】再び図８を参照する。スクランブラ２２によって生成されたＬ種類のスクランブルされた透かしデータＸ’は、ＥＣＣ部２４により誤り訂正のためのパリティを付加された後に、埋め込み部２６によりホストデータＶに埋め込まれる（Ｓ１４）。

【００４７】図７（ａ）、（ｂ）は、スクランブルされた透かしデータＸ’の埋め込み方法を説明する図である。Ｌ種類のスクランブルされた透かしデータＸ’をx^0，x^1，・・・，x^{L-1}　とする。各透かしデータの候補のビット系列は、次式のように表される。先頭のｒビットは識別データである。また、スクランブル処理後のビット０は、－１に置き換えて、以下の処理を行う。

※【００４８】

$$x^0 = \{-1, \cdots, -1, -1, x^0_0, x^0_1, \cdots, x^0_{n-1}\}$$
$$x^1 = \{-1, \cdots, -1, 1, x^1_0, x^1_1, \cdots, x^1_{n-1}\}$$
$$\cdots$$
$$x^{L-1} = \{1, \cdots, 1, 1, x^{L-1}_0, x^{L-1}_1, \cdots, x^{L-1}_{n-1}\}$$

【００４９】ｎビットの透かしデータの埋め込み対象として選択されたホストデータＶのサンプルの集合のペア（V^+，V^-）を次のように定義する。サンプルの集合V^+，V^-は次のようにそれぞれｎ個の要素をもつ。なお、ホストデータＶは、空間軸上のサンプル、時間軸上のサンプル、周波数軸上のサンプル、たとえばＤＣＴ変換、ＦＦＴ変換、ＤＷＴ変換などの処理後のサンプルなどにより表現される。

12

【００５０】

$V^+ = \{v^+_0, v^+_1, \cdots, v^+_{n-1}\}$

$V^- = \{v^-_0, v^-_1, \cdots, v^-_{n-1}\}$

ここでサンプルの集合V^+，V^-の要素である各サブセット

$v^+_i = \{v^+_{i,0}, v^+_{i,1}, \cdots, v^+_{i,m-1}\}$

$v^-_i = \{v^-_{i,0}, v^-_{i,1}, \cdots, v^-_{i,m-1}\}$

【００５２】透かしデータの候補x^k（k＝0，・・・，L－1）をサンプルの集合のペア（V^+，V^-）に次のように埋め込み、L種類の埋め込みホストデータの候補W^kを生成する。

【００５３】

$w^{+k}_{i,j} = v^+_{i,j} + \alpha^+_{i,j} \cdot x^k_i$

$w^{-k}_{i,j} = v^-_{i,j} - \alpha^-_{i,j} \cdot x^k_i$

ここで$\alpha^+_{i,j}$および$\alpha^-_{i,j}$は人間の視覚モデルにもとづいて知覚されるノイズを減少するためのスケーリングパラメータであり、いずれも正の値である。あるいは、$\alpha^+_{i,j}$および$\alpha^-_{i,j}$は、ある確率分布、たとえばガウシアン分布、一様分布などに従うように、秘密鍵Kによって生成される正の値であってもよい。この場合、透かしの埋め込み強度は減少するが、埋め込まれた透かしの秘匿性は向上する。このようにして、k番目の透かしデータの候補の各ビットx^k_iは各サブセットv^+_i、v^-_iのそれぞれm個のサンプルに重複して埋め込まれる。重複の数mが大きいほど、透かしビットが失われる可能性が低くなり、検出誤差が小さくなる一方で、ホストデータに埋め込むことができる透かしのビット数が減少する。$\alpha^+_{i,j}$および$\alpha^-_{i,j}$は、視覚上の劣化を検知できないように各ピクセル毎に設定される値であり、原理的には、埋め込むピクセル数mを増やしても、人間の視覚上、画質の劣化は検知されない。しかし、１ビットを埋め込むのに費やすピクセル数が増加するということは、埋め込み領域には制限があるため、埋め込むことができるビット数が減少することを意味し、したがって埋め込み率の低下を招くことなる。※

＊ットのv^+_i、v^-_iは、次のようにホストデータVのm個のサンプルデータからなる。

【００５１】

$v^+_i = \{v^+_{i,0}, v^+_{i,1}, \cdots, v^+_{i,m-1}\}$

$v^-_i = \{v^-_{i,0}, v^-_{i,1}, \cdots, v^-_{i,m-1}\}$

※【００５４】各サブセットv^+_i、v^-_iは、一例としてホストデータVを離散コサイン変換（Discrete Cosine Transform）したときに得られるＤＣＴブロックであり、透かしビットの埋め込み対象として選ばれるm個のサンプルデータは、ＤＣＴブロックに含まれるm個のＤＣＴ係数である。図７（ａ）、（ｂ）は、８×８のＤＣＴブロックのペアv^+_i、v^-_iのそれぞれm個のＤＣＴ係数に透かしデータx^k_iが埋め込まれる様子を示している。ブロックペアv^+_i、v^-_iおよびm個のＤＣＴ係数は、秘密鍵Kに基づいて選択される。

【００５５】図８に戻り、ＳＮＲ計算部２８は、L種類の埋め込みホストデータの候補W^kに対して透かしデータx^kの耐性、すなわち埋め込み強度を評価し（Ｓ１６）、セレクタ３０は埋め込み強度が最大となる埋め込みホストデータの候補W^kを最終的な埋め込みホストデータWとして選択する（Ｓ１８）。

【００５６】埋め込み強度の評価式を与える前に、埋め込みホストデータWに対して信号処理や画像処理などにより変形が加えられた場合に、透かしデータX’がどのように検出されるかを検討する。埋め込みホストデータWに加えられる変形をノイズNとして扱い、ノイズNが加わった埋め込みホストデータWを埋め込みホスト信号W’と呼ぶ。この埋め込みホスト信号W’から透かしデータX’を抽出する方法を説明する。埋め込みホスト信号の集合のペア（W'^+，W'^-）を次のように定義する。埋め込みホスト信号の集合W'^+，W'^-は次のようにそれぞれn個の要素をもつ。

【００５７】

$W'^+ = \{w'^+_0, w'^+_1, \cdots, w'^+_{n-1}\}$

$W'^- = \{w'^-_0, w'^-_1, \cdots, w'^-_{n-1}\}$

ここで埋め込みホスト信号の集合W'^+，W'^-の要素　★の埋め込み位置に対応して、次のように埋め込みホスト

である各サブセットw'^+_i、w'^-_iは、電子透かし★　信号W’のm個のサンプルデータからなる。

$w'^+_i = \{w'^+_{i,0}, w'^+_{i,1}, \cdots, w'^+_{i,m-1}\}$

$w'^-_i = \{w'^-_{i,0}, w'^-_{i,1}, \cdots, w'^-_{i,m-1}\}$

【００５８】透かしビットx^k_iを検出するために、次☆　☆の判定値z_iを計算する。

$$z_i = \Sigma_{j=0}^{m-1} (w'^+_{i,j} - w'^-_{i,j})$$

$$= \Sigma_{j=0}^{m-1} [(w^+_{i,j} + n^+_{i,j}) - (w^-_{i,j} + n^-_{i,j})]$$

$$= \Sigma_{j=0}^{m-1} [(v^+_{i,j} - v^-_{i,j}) + (\alpha^+_{i,j} + \alpha^-_{i,j}) \cdot x^k_i + (n^+_{i,j} - n^-_{i,j})]$$

ここで$\Sigma_{j=0}^{m-1}(v^+_{i,j} - v^-_{i,j})$はm　z_iは$\Sigma_{j=0}^{m-1}[(\alpha^+_{i,j} + \alpha^-_{i,j}) \cdot x^k_i]$の値で近似できる。（$\alpha^+_{i,j}$＋　が十分に大きいとき、一般にガウス分布に従い、０に近づく。またノイズの項$\Sigma_{j=0}^{m-1}(n^+_{i,j} - n$　$\alpha^-_{i,j}$）は正であるから、透かしビットx^k_iが１$^-_{i,j}$）についても同様に０に近づく。したがって、　ならばz_iは正であり、透かしビットx^k_iが－１なら

ばｚｉ は負である。したがってｚｉ の正負により透かしビットｘ^{k}ｉ の値を判定することができる。

【００５９】埋め込み強度の評価は、ホストデータＶを透かしデータＸに対するノイズとみなして、埋め込まれた透かしデータｘ^{k} に対して検出される透かしデータの＊

$$K=arg\max_k (P_k/(2\sigma_k^2))$$

$$P_k=\Sigma_{i=0}^{n-1}|\Sigma_{j=0}^{m-1}(w^{+k}_{i,j}-w^{-k}_{i,j})|^2/n$$

$$\sigma_k^2=\Sigma_{i=0}^{n-1}|\Sigma_{j=0}^{m-1}(w^{+k}_{i,j}-w^{-k}_{i,j})-P_k^{1/2}\cdot x^k_i|^2/n$$

【００６１】透かしビットｘ^{k}ｉ が｛１，－１｝のいずれであるかを判定するための前述の判定値ｚｉ は、埋め込みホストデータＷにノイズが付加される前の状態では、$z_i=\Sigma_{j=0}^{m-1}(w^{+k}_{i,j}-w^{-k}_{i,j})$で与えられることを考慮すると、分散σ$_{k}^{2}$は、判定値ｚｉ により検出される透かしビットと実際に埋め込まれた透かしビットｘ^{k}ｉ の差をｉ＝０，・・・，ｎ－１について評価して合計したものであると言える。一方、Ｐｋ は判定値ｚｉ のｉ＝０，・・・，ｎ－１についての自乗和である。したがって、埋め込まれた透かしデータｘ^{k}と抽出される透かしデータとの間のハミング距離もしくはユークリッド距離が小さく、透かしビットを検出するための判定値の絶対値が大きいほど、Ｐｋ／（２σ$_{k}^{2}$）の値は大きくなる。言い換えれば、Ｐｋ／（２σ$_{k}^{2}$）が最大となる候補を選択することは、透かしビットの検出誤差が最小である候補を選択することを意味する。

【００６２】判定値ｚｉ について、ｖ$^{+}_{i,j}$＞ｖ$^{+}_{i,j}$かつｘ^{k}ｉ ＝１ならばｚｉ ＞＞０となり、ｖ$^{+}$

＊分散を計算することにより行われる。分散が小さいほど、耐性が強いと考えることができる。埋め込みホストデータの候補のペア（Ｗ$^{+k}$，Ｗ$^{-k}$）に対して次式により分散を評価して、最適な候補Ｋを選択する。

【００６０】

$$K=arg\max_k (P_k/(2\sigma_k^2))$$

$$P_k=\Sigma_{i=0}^{n-1}|\Sigma_{j=0}^{m-1}(w^{+k}_{i,j}-w^{-k}_{i,j})|^2$$

$$\sigma_k^2=\Sigma_{i=0}^{n-1}|\Sigma_{j=0}^{m-1}(w^{+k}_{i,j}-w^{-k}_{i,j})-P_k^{1/2}\cdot x^k_i|^2/n$$

※ｉ，ｊ＜ｖ$^{+}_{i,j}$かつｘ^{k}ｉ ＝－１ならばｚｉ ＜＜０となる。したがって前述の評価により最適な透かしデータｘ^{k}の候補を選択することは、判定値ｚｉ による透かしビットｘ^{k}ｉ の検出性能を向上させるために、ｖ$^{+}$ｉ，ｊ＞ｖ$^{+}_{i,j}$ならばｘ’ｉ ＝１となり、ｖ$^{+}_{i,j}$＜ｖ$^{+}_{i,j}$ならばｘ’ｉ ＝－１となるように、元の透かしビットｘｉ をｘ’ｉ に変更することを意味する。これがＧＳ方式のガイディングルールであり、これにより判定値ｚｉ のレスポンスが改善する。

【００６３】復号装置４０の抽出部４２は、ノイズの付加された埋め込みホスト信号Ｗ’を受け取ると、ＥＣＣ復号部４４が硬入力の復号器で構成される場合には、判定値ｚｉ を次のように計算し、判定値ｚｉ の正負で、透かしビットｘ’が｛－１，１｝のいずれであるかを判定し、透かしデータＸ’を得る。また、ＥＣＣ復号部４４が軟入力の復号器で構成される場合には、判定値ｚｉ を｛－１，１｝に硬判定することなく、そのまま、ＥＣＣ復号部４４に送る。

【００６４】

$$z_i=\Sigma_{j=0}^{m-1}(w'^{+}_{i,j}-w'^{-}_{i,j})$$

$$=\Sigma_{j=0}^{m-1}[(w^{+}_{i,j}+n^{+}_{i,j})-(w^{-}_{i,j}+n^{-}_{i,j})]$$

$$=\Sigma_{j=0}^{m-1}[(v^{+}_{i,j}-v^{-}_{i,j})+(\alpha^{+}_{i,j}+\alpha^{-}_{i,j})\cdot x'_i+(n^{+}_{i,j}-n^{-}_{i,j})]$$

【００６５】抽出された透かしデータＸ’はさらにＥＣＣ復号部４４により誤り訂正がなされ、デスクランブラ４６によりスクランブルを解除され、元の透かしデータＸが得られる。

【００６６】以上述べたように、実施の形態によれば、ＧＳ方式を用いて、電子透かしを埋め込む画像や音声などのメディアデータが与えられると、透かしビット系列をそのメディアデータに埋め込みやすいビット系列に変換した上で埋め込むことができる。したがって信号処理、幾何変換、圧縮、データの改ざんなどに対する電子透かしの耐性を強化することができ、透かしの検出精度が大幅に改善する。

【００６７】上記の実施の形態では、図２で示したように、Ｌ種類の透かしデータの候補を生成するために、Ｌ個のマルチプレクサ２０、スクランブラ２２、ＥＣＣ部２４、埋め込み部２６、およびＳＮＲ計算部２８が並列に設けられたが、これらの部材を単一構成にして、Ｌ種類の透かしデータの候補を逐次的に生成、評価して最適な候補を選択してもよい。

【００６８】図９は、そのような逐次型の電子透かしの埋め込み手順を説明するフローチャートである。変数ｉを１に初期化する（Ｓ２０）。マルチプレクサ２０は、暗号化部１２により暗号化された透かしデータＸの先頭にｉ番目の初期データを挿入して符号系列を生成し（Ｓ２２）、スクランブラ２２は、その符号系列をスクランブルして、ｉ番目のスクランブルされた透かしデータＸ’を生成する（Ｓ２４）。スクランブラ２２によって生成されたｉ番目のスクランブルされた透かしデータＸ’は、必要に応じてＥＣＣ部２４により誤り訂正のためのパリティを付加された後に、埋め込み部２６によりホストデータＶに埋め込まれる（Ｓ２６）。ＳＮＲ計算部２８は、ｉ番目の埋め込みホストデータの候補Ｗ^{i}に

対して透かしデータx^iの耐性、すなわち埋め込み強度S_iを評価する（Ｓ２８）。セレクタ３０は、埋め込み強度S_iが最低の評価値を保証する基準値Ｔより大きいかどうかを判定する（Ｓ３０）。もし埋め込み強度S_iが基準値Ｔより大きければ（Ｓ３０のＹ）、変数Ｋに現在の変数ｉの値を代入し（Ｓ３２）、Ｋ番目の埋め込みホストデータの候補を最終的な埋め込みホストデータＷとして選択する（Ｓ４０）。埋め込み強度S_iが基準値Ｔ以下の場合（Ｓ３０のＮ）、現在の変数ｉの値がＬに等しいなら（Ｓ３４のＹ）、これまで調べた埋め込み強度S_kの値が最大となる添え字ｋを変数Ｋに代入し（Ｓ３８）、Ｋ番目の埋め込みホストデータの候補を最終的な埋め込みホストデータＷとして選択する（Ｓ４０）。現在の変数ｉの値がＬより小さいなら（Ｓ３４のＮ）、変数ｉを１だけインクリメントして（Ｓ３６）、ステップＳ２２に戻る。

【００６９】この繰り返し処理により、埋め込み強度が所望の基準値以上である候補が得られた時点で、その候補を最終的な埋め込みホストデータＷとして選択し、そのような候補が生成されなければ、Ｌ個の埋め込みホストデータの候補を生成して、その中から埋め込み強度が最大であるものを最終的な埋め込みホストデータＷとして選択することができる。

【００７０】実施の形態２

$$K=\mathrm{argmax}_k\ (P_k/(2\sigma_k^{\,2}))$$

$$P_k=\Sigma_{i=0}^{n-1}\left|\Sigma_{j=0}^{m-1}(w^{*+k}_{i,j}-w^{*-k}_{i,j})\right|^2/n$$

$$\sigma_k^{\,2}=\Sigma_{i=0}^{n-1}\left|\Sigma_{j=0}^{m-1}(w^{*+k}_{i,j}-w^{*-k}_{i,j})-P_k^{1/2}\cdot x^k_i\right|^2/n$$

ここで$w^{*+k}_{i,j}$、$w^{*-k}_{i,j}$は特定の処理がなされた後の埋め込みホストデータＷである。特定の処理がたとえばＪＰＥＧ圧縮であると分かっている場合、※

$$w^{*+k}_{i,j}=\mathrm{round}(w^{+k}_{i,j}/q_{i,j})\cdot q_{i,j}$$

$$w^{*-k}_{i,j}=\mathrm{round}(w^{-k}_{i,j}/q_{i,j})\cdot q_{i,j}$$

ここで$q_{i,j}$は位置（ｉ，ｊ）におけるＪＰＥＧの量子化テーブルの値である。ｒｏｕｎｄはＪＰＥＧ圧縮時に用いられる四捨五入の演算を行う関数である。

【００７４】本実施の形態によれば、透かしの埋め込み時に、埋め込み後のホストデータに対する特定の処理を想定して埋め込み強度を評価し、埋め込み強度の高い透かしデータのビット系列を選択するため、特定の処理に対する耐性の強い電子透かし埋め込みデータを生成することができる。

【００７５】実施の形態３

図１２は、実施の形態３に係る符号化装置５０の構成を示す。この符号化装置５０は、透かしデータＸをホストデータＶの複数の埋め込み位置の候補に埋め込み、透かしの耐性が強くなる候補を選択して、最終的な埋め込みホストデータＷとして出力する。実施の形態１と共通する構成については同一符号を付して説明を省き、実施の

＊図１０は実施の形態２に係る符号化装置１１の構成を示す。本実施の形態では、電子透かしの埋め込まれたホストデータＶが受ける圧縮符号化などの特定の処理をあらかじめ想定し、透かしの埋め込み時にその特定の処理による影響を考慮して、電子透かしに耐性をもたせる。実施の形態１と共通する構成については同一符号を付して説明を省き、実施の形態１とは異なる構成と動作について説明する。

【００７１】変更部１５は、透かしデータＸをスクランブルする際、ホストデータＶが受ける特定の処理による歪みＤを考慮して耐性の強い透かしデータのビット系列を選択し、スクランブルされた透かしデータＸ’を出力する。図１１は変更部１５と埋め込み部１６の機能構成図である。重みつきＳＮＲ計算部２９は、Ｌ種類のスクランブルされた透かしデータX'_cが埋め込まれたホストデータＷの候補について、透かしデータＸの耐性を評価する際に、特定の処理により想定される歪みＤを考慮に入れる。具体的には、埋め込まれた透かしデータと検出される透かしデータとの間の分散により埋め込み強度を評価する際に、埋め込みホストデータＷに対する特定の処理による劣化を考慮した以下の重み付け分散を用いる。

【００７２】

※

$$K=\mathrm{argmax}_k\ (P_k/(2\sigma_k^{\,2}))$$

$$P_k=\Sigma_{i=0}^{n-1}\left|\Sigma_{j=0}^{m-1}(w^{*+k}_{i,j}-w^{*-k}_{i,j})\right|^2/n$$

$$\sigma_k^{\,2}=\Sigma_{i=0}^{n-1}\left|\Sigma_{j=0}^{m-1}(w^{*+k}_{i,j}-w^{*-k}_{i,j})-P_k^{1/2}\cdot x^k_i\right|^2/n$$

※$w^{*+k}_{i,j}$、$w^{*-k}_{i,j}$はＪＰＥＧの量子化テーブルを用いて次式により計算することができる。

【００７３】

$$w^{*+k}_{i,j}=\mathrm{round}(w^{+k}_{i,j}/q_{i,j})\cdot q_{i,j}$$

$$w^{*-k}_{i,j}=\mathrm{round}(w^{-k}_{i,j}/q_{i,j})\cdot q_{i,j}$$

形態１とは異なる構成と動作について説明する。

【００７６】位置検出部５２は、スクランブルされた埋め込み位置Ｐを生成し、埋め込み部５４は、秘密鍵Ｋを用いて、ホストデータＶの埋め込み位置Ｐに透かしデータＸを埋め込み、埋め込みホストデータＷを出力する。位置検出部５２と埋め込み部５４は協同して、複数の埋め込み位置Ｐを生成し、それぞれの埋め込み位置Ｐに透かしデータＸを埋め込み、複数の埋め込みホストデータＷの候補を生成し、それらの候補の一つを選択する機能をもつ。

【００７７】図１３は位置検出部５２と埋め込み部５４の機能構成図である。ＥＣＣ部２４は透かしデータX_bに誤り訂正のためのパリティを付加した透かしデータX_cを生成する。位置情報生成部６０は、ホストデータＶについてＬ個の埋め込み位置Ｐの候補を生成する。埋め込み部２６はＬ個の埋め込み位置Ｐの候補のそれぞれに

透かしデータＸｃを埋め込み、Ｌ種類の埋め込みホストデータWの候補を生成する。

【００７８】位置情報生成部６０は、ＧＳ方式によりＬ個のスクランブルされた埋め込み位置Ｐの候補を生成する。初期埋め込み位置P^*に対して、Ｌ種類の初期データ$C_0 \sim C_{L-1}$を与えて、実施の形態１に述べた方法により、初期埋め込み位置P^*をスクランブルする。

【００７９】図１４は、実施の形態３に係る復号装置の構成を示す。この復号装置は、埋め込みホスト信号W'から埋め込まれた透かしデータＸｃを抽出し、この透かしデータＸｃに対して誤り復号し、誤り訂正がなされた透かしデータＸｂを得る処理を行う。位置情報生成部６０は、図１３に示した符号化装置５０における位置情報生成部６０と同様に、Ｌ個の埋め込み位置Ｐの候補を生成する。Ｌ個の抽出部４２は、位置情報生成部６０により与えられたＬ個の埋め込み位置Ｐの候補から、埋め込みホスト信号W'に埋め込まれたＬ種類の透かしデータＸｃの候補を抽出する。Ｌ個の埋め込み位置Ｐの候補の内、一つの候補が正しい埋め込み位置である。整合フィルタ６２は、Ｌ種類の透かしデータＸｃの候補と、想定される透かしデータＹとの間で相関を計算し、マッチングをとる。セレクタ６４が相関の最も高い透かしデータＸｃの候補を選択することで、正しい埋め込み位置にある透かしデータＸｃが得られる。さらに透かしデータＸｃは、ＥＣＣ復号部４４により誤り訂正がなされる。

【００８０】想定される透かしデータＹは、ホストデータVに埋め込まれた透かしデータＸがあらかじめわかっている場合に与えられる。たとえば、ホストデータVの作成者があらかじめわかっており、その作成者の透かしデータＸがホストデータVに埋め込まれているかどうかを確認する場合がある。一般に、本実施の形態は、埋め込まれている電子透かし情報があらかじめ想定されているが、透かしデータの埋め込み位置が候補としてしか与えられていない場合に適用することができる。

【００８１】本実施の形態によれば、電子透かしを埋め込む対象となるメディアデータが与えられると、そのメディアデータに応じて、透かしデータを埋め込み易い位置を検出して、透かしデータを埋め込むことができ、埋め込まれる透かしの耐性を強化することができる。

【００８２】実施の形態４

実施の形態１から３において、透かしデータＸの誤り訂正のためにＥＣＣが用いられた。復号側で透かしビット$x^k{}_i$を検出する際、判定値z_iが利用されていた点を考慮すると、透かしデータの検出には、ビットの値の確からしさを示す補助情報を復号判定に用いる軟判定復号が有効であることが理解される。本実施の形態では、そのような軟判定復号法としてターボ符号を用い、符号化側のＥＣＣ部２４、復号側のＥＣＣ復号部４４の代わりに、それぞれ図１５のターボ符号化部７０、図１６のターボ復号部９０を用いる。

【００８３】図１５を参照してターボ符号化部７０の構成と動作を説明する。符号化の対象として入力されるユーザビット列ＵＢは、第１符号化器７２に入力され、パリティビット列P_0が生成される。ユーザビット列ＵＢはインターリーバ７４により順序が並べ替えられて、第２符号化器７６に入力され、パリティビット列P_1が生成される。２つのパリティビット列P_0、P_1はマルチプレクサ・パンクチャラ７８により、間引き（puncture）されながら多重化され、さらにユーザビット列ＵＢと多重化されて符号化ビットＣＢとして出力される。なお、パンクチャの処理は、埋め込みビット数を増加させたいときに用いられるオプショナルな処理であり、必要でない場合は省略してもよい。

【００８４】図１６を参照してターボ復号部９０の構成と動作を説明する。図１５の第１符号化器７２に対応する第１軟復号器９２は、受信したチャネル出力ＣＯを復号し、各情報シンボルの復号結果とそれに対する信頼度の情報を与える外部情報（Extrinsic Information）を出力する。ここで、受信したホストデータから判定値として抽出される軟値z_iがチャネル出力ＣＯとして扱われる。図１５の第２符号化器７６に対応する第２軟復号器９８は、第１軟復号器９２からインターリーバ９４を介して得た外部情報を事前確率として用いて、インターリーバ９６により順序を並べ替えられたチャネル出力ＣＯの復号処理を行い、復号結果に対する外部情報をデインターリーバ１００を介して第１軟復号器９２に与える。第１軟復号器９２は第２軟復号器９８からの外部情報を事前確率として用いて、チャネル出力ＣＯの復号処理を行う。この一連の動作を繰り返し行うことで、ターボ復号部９０は最終判定ＦＤを出力する。インターリーバ９４、９６による並べ替えは、図１５のインターリーバ７４の並べ替えと同じである。またデインターリーバ１００はインターリーバ９４、９６の並べ替えを元に戻す処理を行う。

【００８５】ターボ復号部９０では、第１符号化器７２と第２符号化器７６が、互いに他方から提供される事前情報を利用し合って、ＭＡＰ（Maximum A posteriori Probability）復号による復号結果を逐次的に改善することができる。これにより透かしビットを検出する際のビット誤り率（ＢＥＲ）をさらに低減することができる。

【００８６】以上、本発明を実施の形態をもとに説明した。これらの実施の形態は例示であり、それらの各構成要素や各処理プロセスの組み合わせにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【００８７】そのような変形例として、実施の形態２における特定の処理を想定して埋め込み強度を評価する方法は、実施の形態３における埋め込み強度の評価の際にも適用することができる。

【００８８】複数の透かしデータの候補または埋め込み

位置の候補を生成するために、多様性に富んだ候補の生成が可能なＧＳ方式を用いたが、他のスクランブル方式を適用してもよく、また何らかの方法でランダムに候補のデータを生成してもよい。また実施の形態では、逆スクランブルにより、生成された透かしデータの候補から元の透かしデータを再現したが、生成された透かしデータの候補と元の透かしデータとを対応づけたテーブルを備え、このテーブルを参照して元の透かしデータを求めてもよい。

【００８９】またスクランブルの際に初期データとして使用した識別データは、透かしデータの先頭に挿入されて復号側に提供されていたが、この識別データを透かしには埋め込まずに、符号化側で秘密鍵として保持、管理してもよい。その場合、復号側はこの秘密鍵を取得した上で、透かしデータのスクランブルを解除する。また実施の形態３では、復号側でこの識別データを秘密鍵として入手する場合は、埋め込み位置が秘密鍵から特定されるため、整合フィルタ６２による埋め込み位置の検出作業が不要となり、したがってあらかじめ想定される透かしビットを用意しておく必要もなくなる。

【００９０】また実施の形態４ではターボ符号を説明したが、軟判定の可能な誤り訂正符号であれば他の符号化方法を用いてもよい。

【００９１】なお、実施の形態１の変形として、逐次型の候補の生成、評価のための構成と動作を説明したが、同様の逐次型の構成と動作が、実施の形態２および３にも適用できることはいうまでもない。

【００９２】実施の形態３では、埋め込み位置の候補をスクランブル方式により生成したが、埋め込み位置の候補を次に述べるテーブルマッチングによりランダムに生成してもよい。このために、電子透かしの埋め込み側と抽出側は、埋め込み位置の候補を識別するための識別データと埋め込む位置とを対応づけたテーブルを備える。このテーブルは、透かしデータの第１ビットについて、たとえば、「識別番号０の場合は（１，２９）の位置、識別番号１の場合は（９８３，２５１）の位置、・・・、識別番号１５の場合は（５４２，３７）の位置に埋め込む」といった識別番号と埋め込み座標との対応関係を格納する。第２番目から第ｎ番目のビットについてもそれぞれ埋め込み位置が異なる対応関係が格納される。埋め込み位置は何らかの方法でランダムに生成される。埋め込み側では、このテーブルを参照して、埋め込み位置の候補の識別データに対応づけて埋め込み位置の候補を生成し、透かしデータをその候補の位置に埋め込む。抽出側では、埋め込み位置の候補の識別データにもとづいてこのテーブルを参照することにより、埋め込み位置を特定し、透かしデータをその位置から抽出する。この方法によれば、埋め込み位置のランダム性が十分に保証され、頑強な埋め込みを実現することができる。また抽出側では、埋め込み位置の候補の識別データ以外にこのテーブルをもっていなければ、埋め込み位置を知ることができないため、セキュリティを高めることができる。

【発明の効果】本発明によれば、電子透かしの耐性が向上し、透かしの検出精度が改善する。

【図面の簡単な説明】

【図１】　実施の形態１に係る符号化装置の構成図である。

【図２】　図１の変更部と埋め込み部の機能構成図である。

【図３】　実施の形態１に係る復号装置の構成図である。

【図４】　元の透かしデータとＬ種類のスクランブルされた透かしデータとの関係を説明する図である。

【図５】　符号化時の畳み込み演算を説明する図である。

【図６】　復号時の畳み込み演算を説明する図である。

【図７】　図７（ａ）、（ｂ）は、スクランブルされた透かしデータの埋め込み方法を説明する図である。

【図８】　符号化装置による電子透かしの埋め込み手順を説明するフローチャートである。

【図９】　符号化装置による別の電子透かしの埋め込み手順を説明するフローチャートである。

【図１０】　実施の形態２に係る符号化装置の構成図である。

【図１１】　図１０の変更部と埋め込み部の機能構成図である。

【図１２】　実施の形態３に係る符号化装置の構成図である。

【図１３】　図１２の位置検出部と埋め込み部の機能構成図である。

【図１４】　実施の形態３に係る復号装置の構成図である。

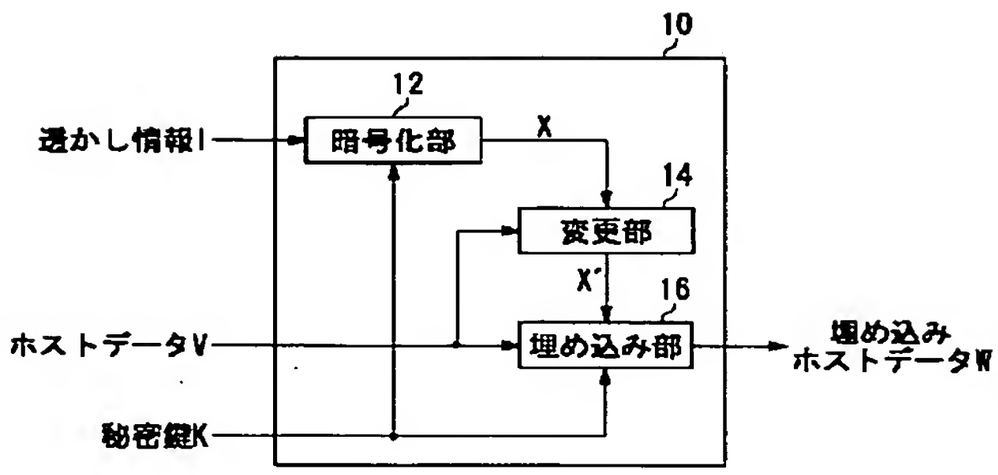
【図１５】　実施の形態４に係る符号化装置のターボ符号化部の構成図である。

【図１６】　実施の形態４に係る符号化装置のターボ復号部の構成図である。

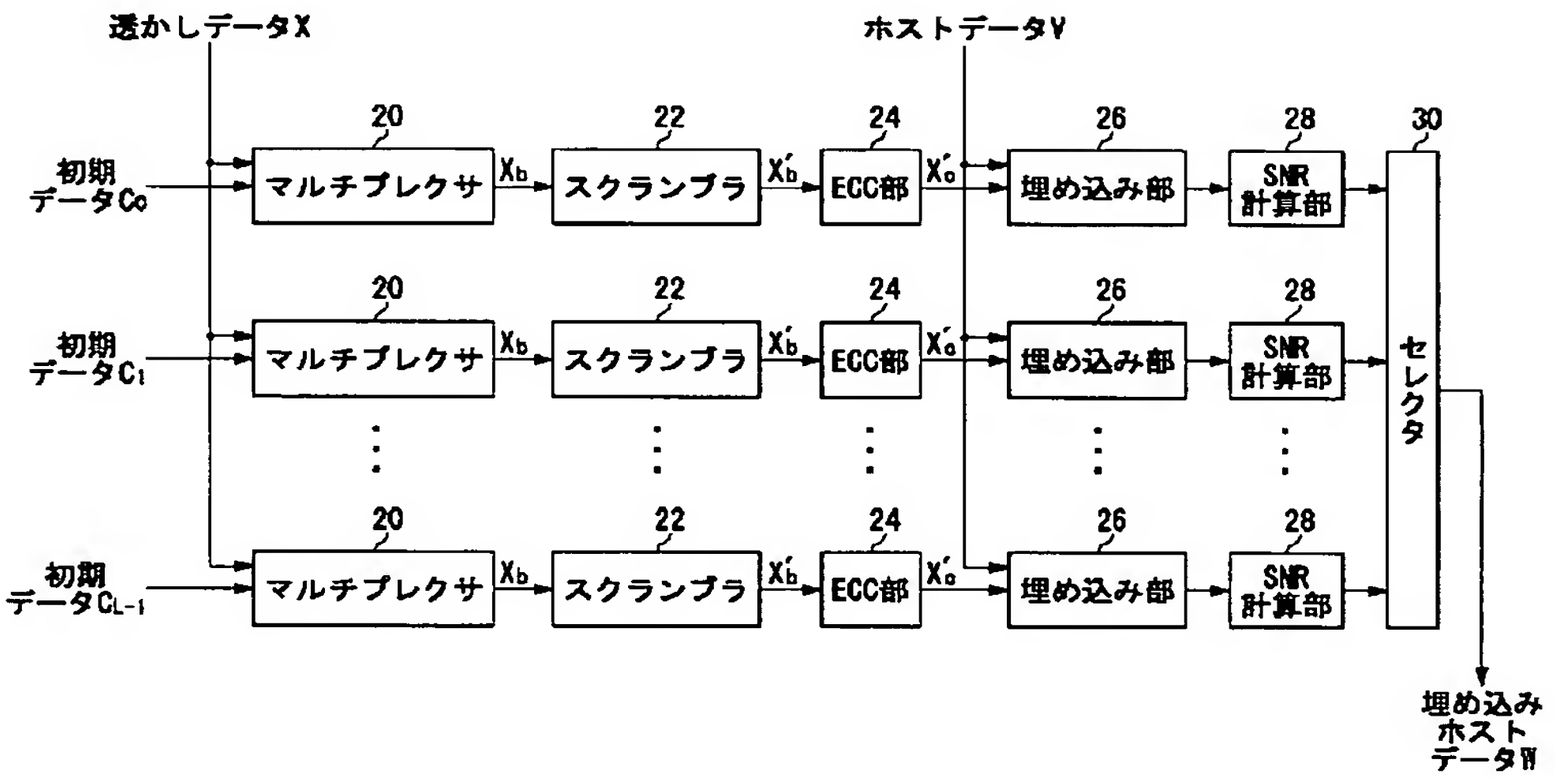
【符号の説明】

１０　符号化装置、　１２　暗号化部、　１４　変更部、　１６　埋め込み部、　２０　マルチプレクサ、　２２　スクランブラ、　２４　ＥＣＣ部、　２６埋め込み部、　２８　ＳＮＲ計算部、　２９　重みつきＳＮＲ計算部、　３０セレクタ、　４０　復号装置、　４２　抽出部、　４４　ＥＣＣ復号部、　４６　デスクランブラ、　５０　符号化装置、　５２　位置検出部、　５４　埋め込み部、　６０　位置情報生成部、　６２　整合フィルタ、　６４　セレクタ、７０　ターボ符号化部、　９０　ターボ復号部。

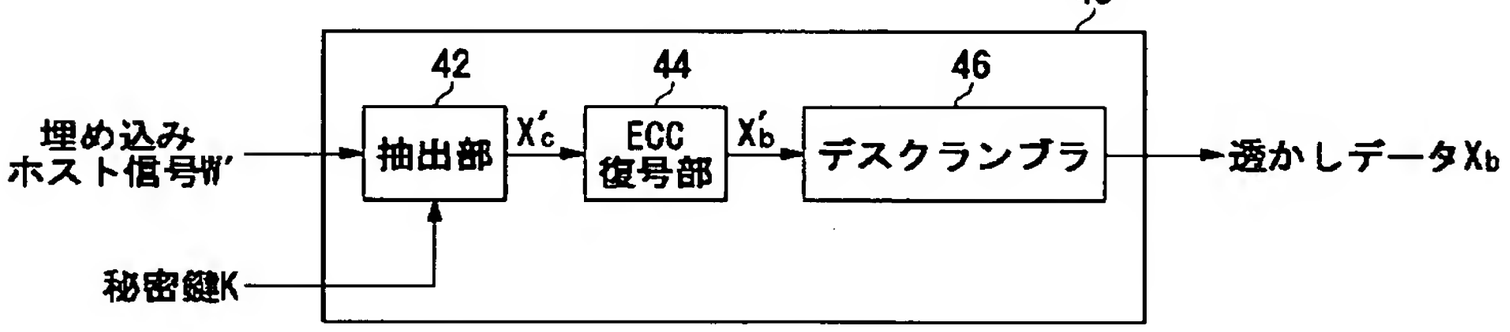
【図１】


10
12
透かし情報I
暗号化部
X
14
変更部
X'
16
ホストデータV
埋め込み部
埋め込み
ホストデータW
秘密鍵K

【図２】


透かしデータX
ホストデータV
20
22
24
26
28
30
初期
データC0
初期
データC1
初期
データCL-1
マルチプレクサ
Xb
スクランブラ
X'b
ECC部
X'c
埋め込み部
SNR
計算部
セレクタ
埋め込み
ホスト
データW

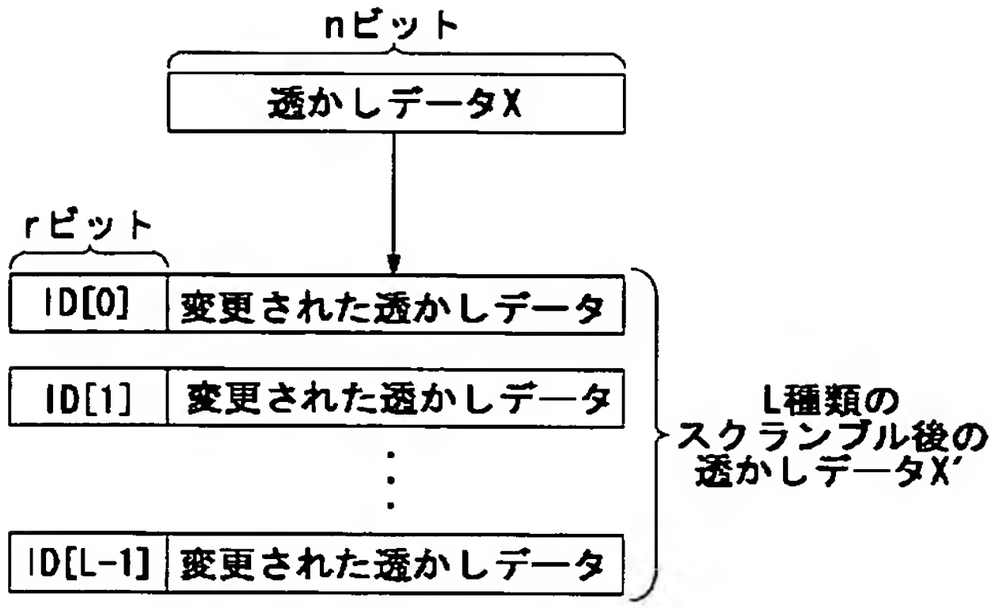
【図３】


42
44
46
埋め込み
ホスト信号W'
抽出部
X'c
ECC
復号部
X'b
デスクランブラ
透かしデータXb
秘密鍵K

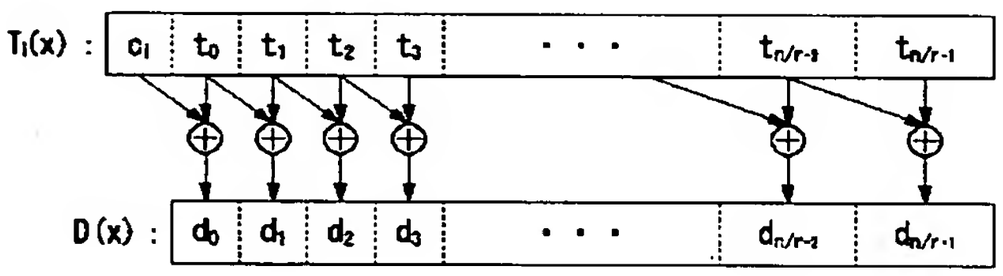
【図５】

D(x) :
d0
d1
d2
d3
・・・
dn/r-2
dn/r-1
Ti(x) :
ci
t0
t1
t2
t3
・・・
tn/r-2
tn/r-1
rビット

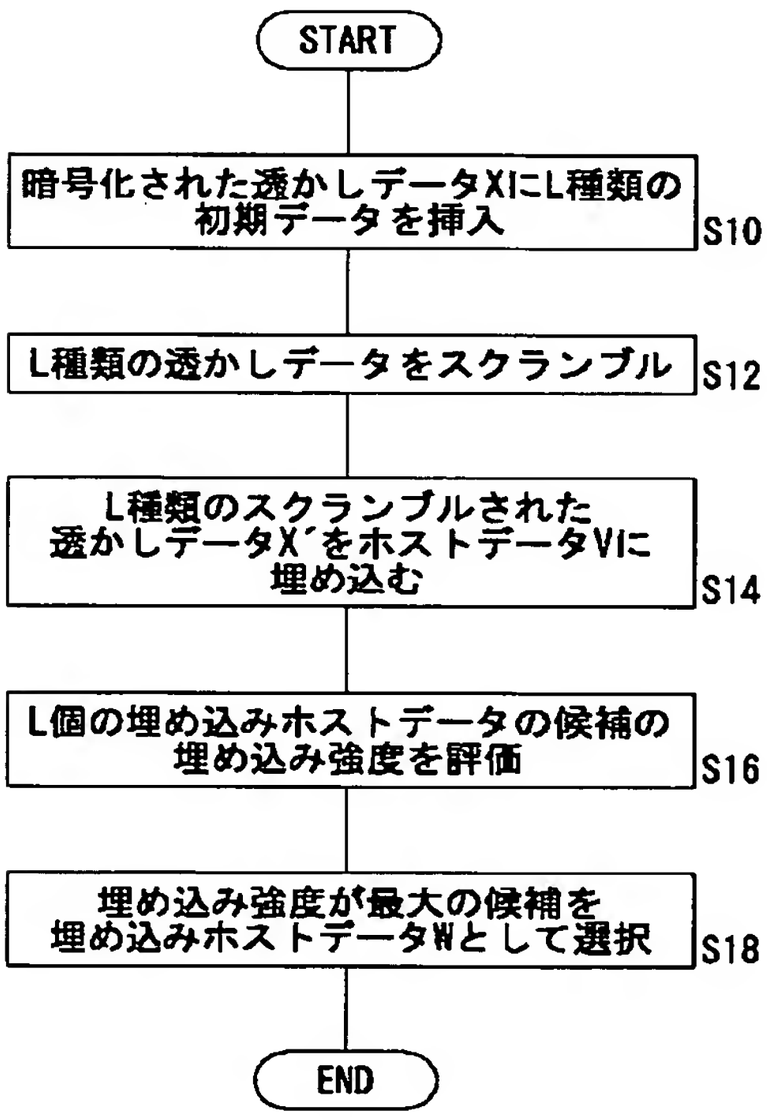
【図４】



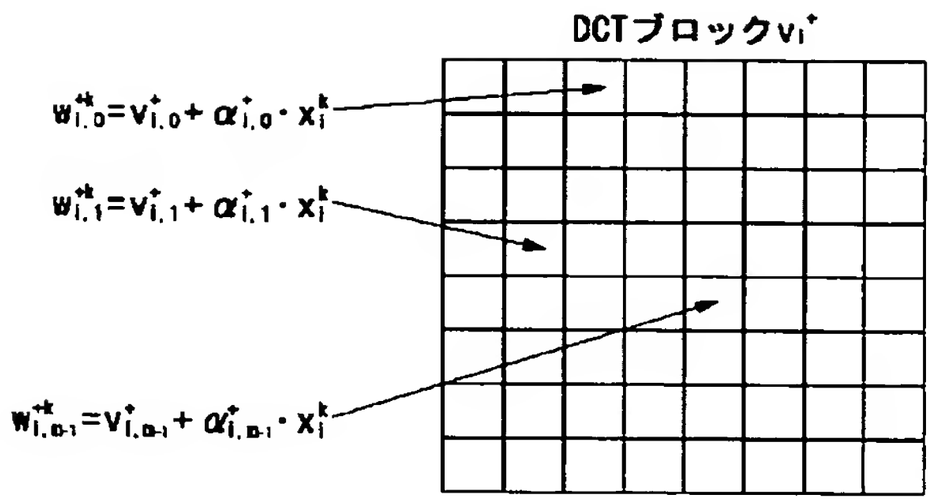
【図６】



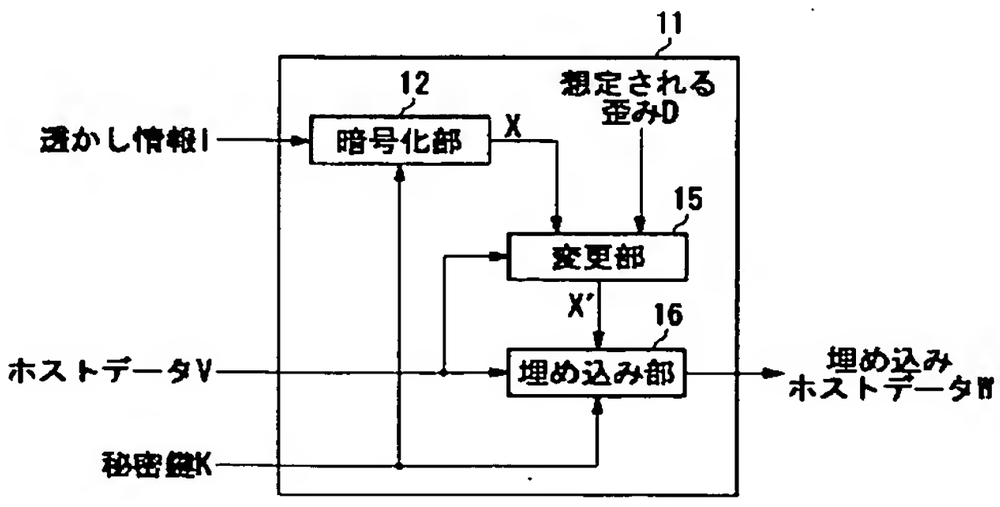
【図８】



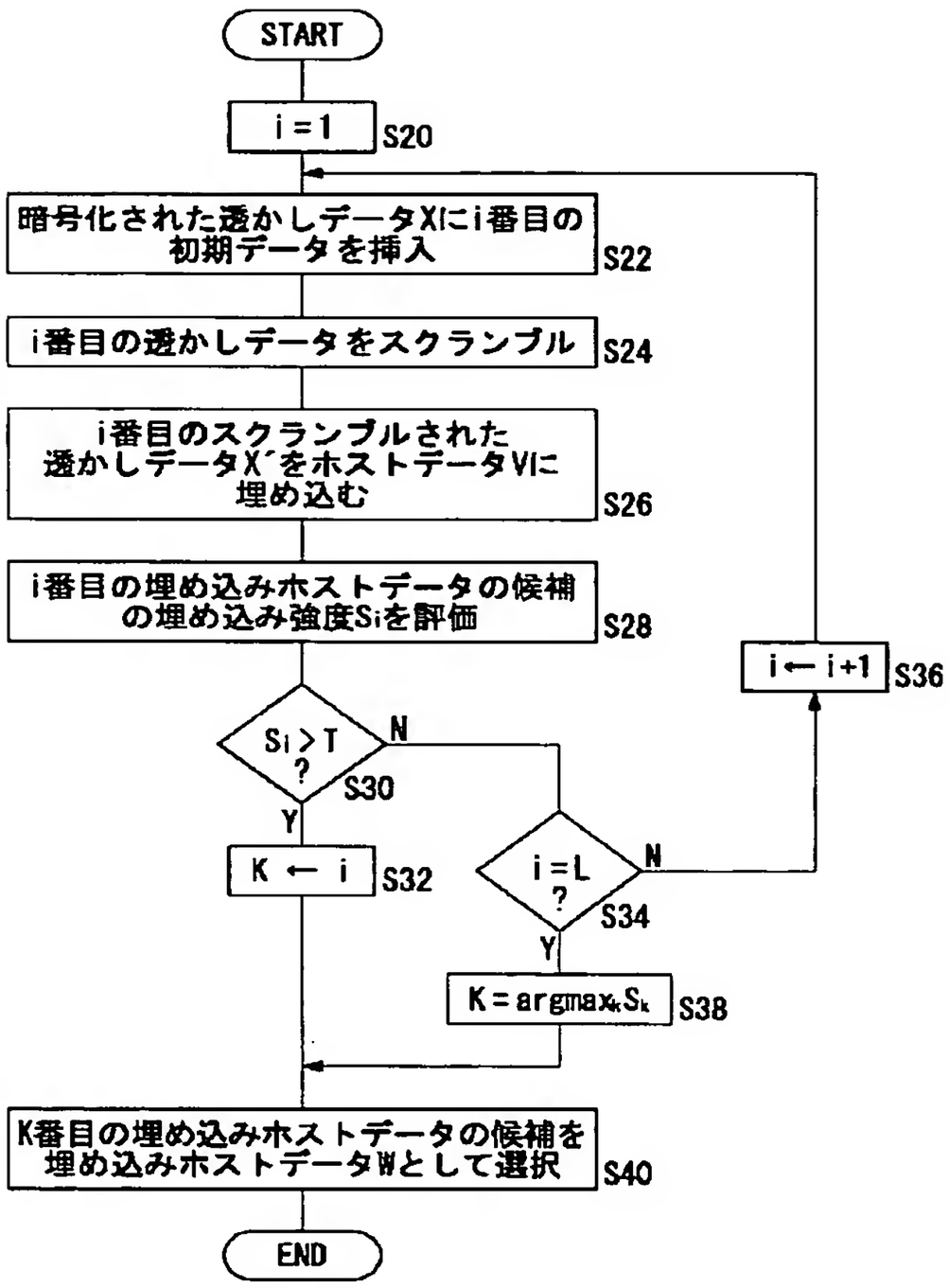
【図７】



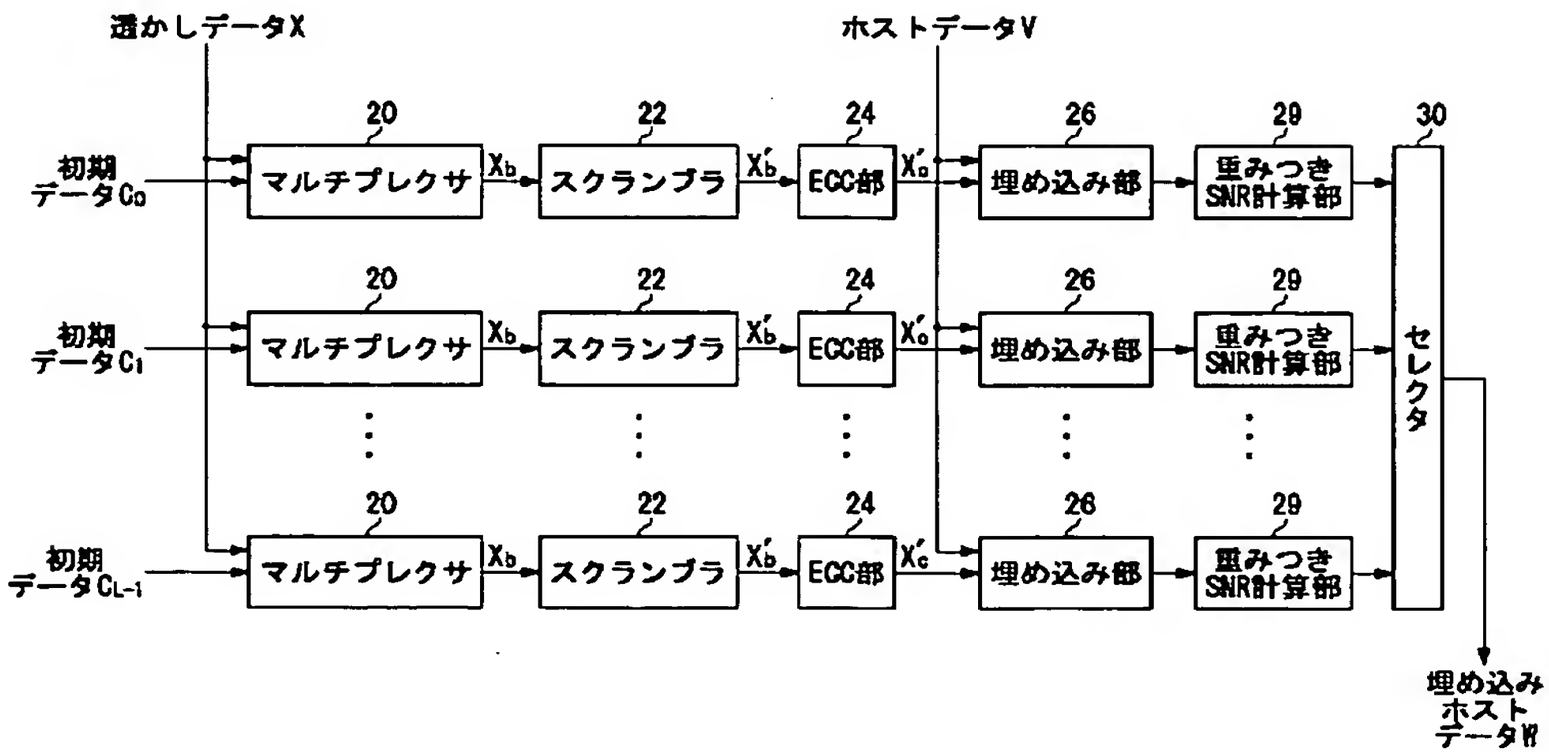
【図１０】



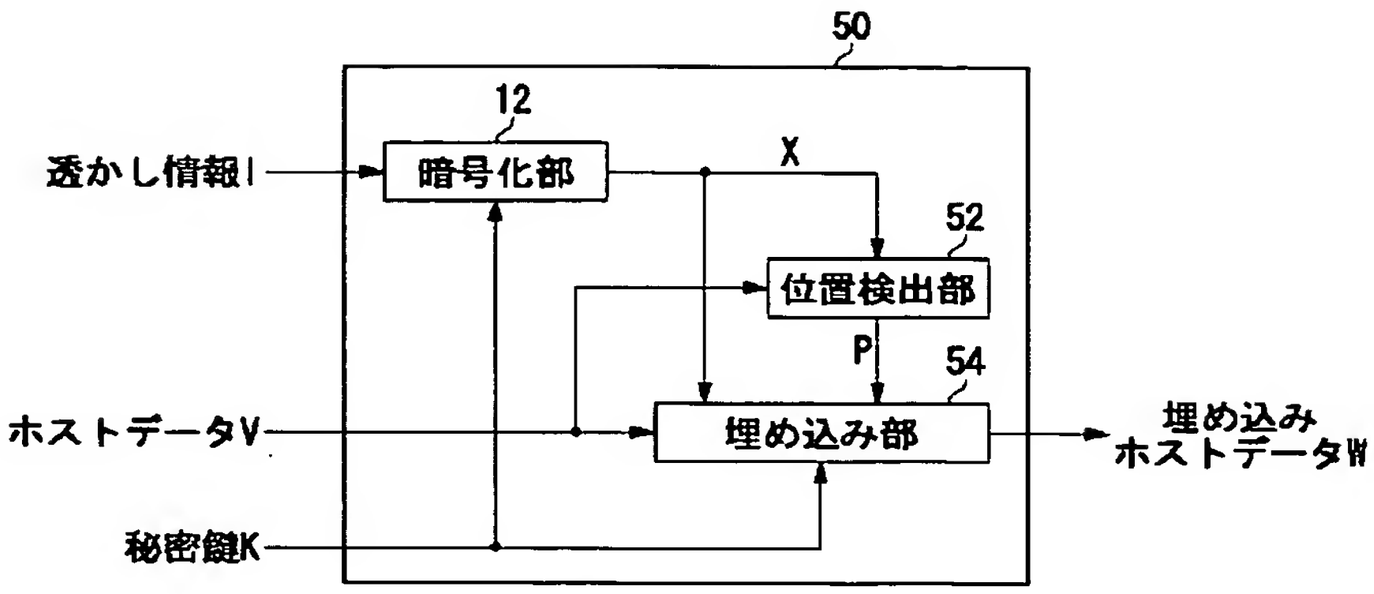
【図９】


START
i＝1
S20
暗号化された透かしデータXにi番目の初期データを挿入
S22
i番目の透かしデータをスクランブル
S24
i番目のスクランブルされた透かしデータX′をホストデータVに埋め込む
S26
i番目の埋め込みホストデータの候補の埋め込み強度Siを評価
S28
Si＞T ?
S30
N
Y
K ← i
S32
i＝L ?
S34
N
Y
i ← i+1
S36
K＝argmaxkSk
S38
K番目の埋め込みホストデータの候補を埋め込みホストデータWとして選択
S40
END

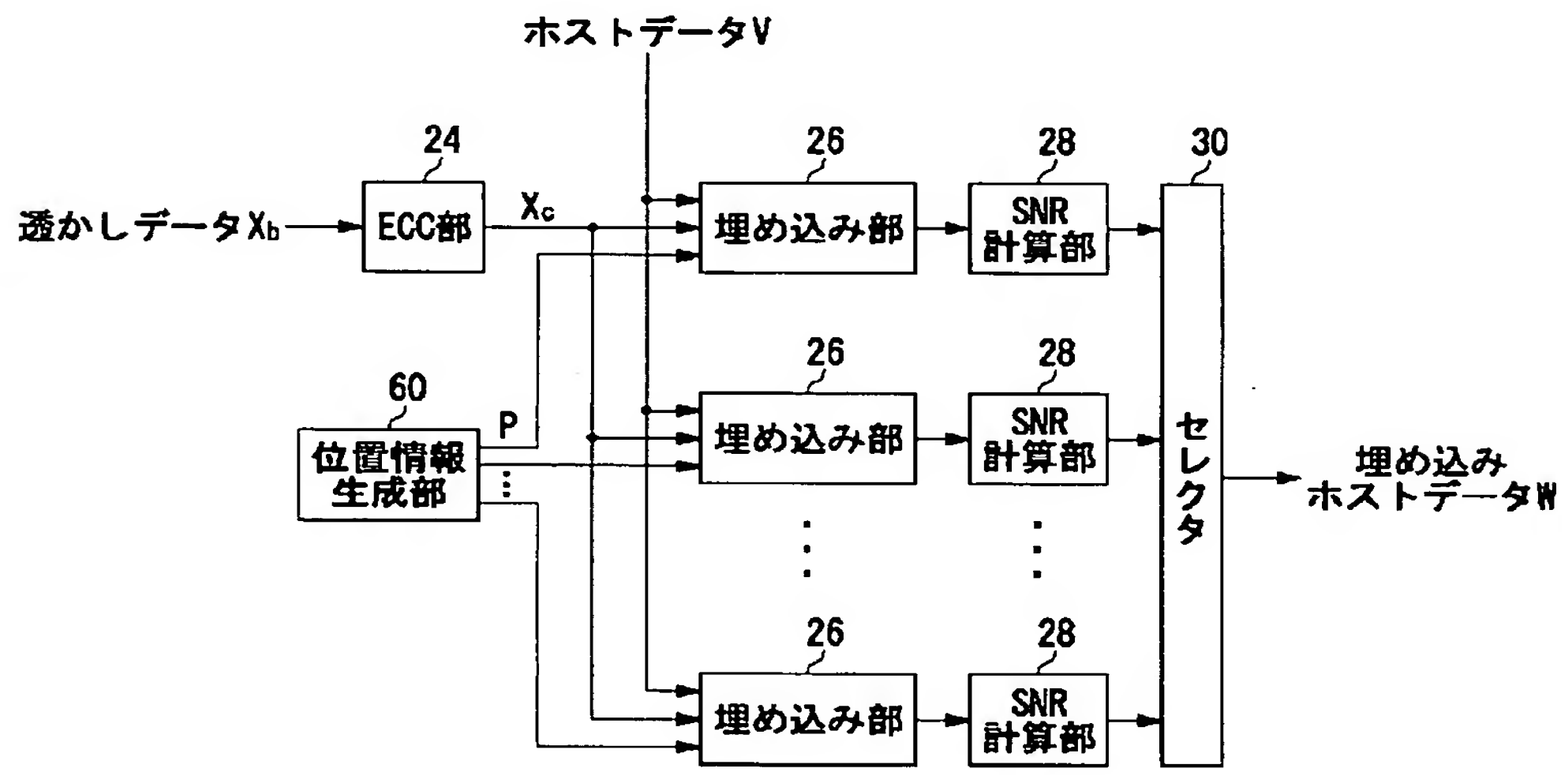
【図１１】


透かしデータX
ホストデータV
初期データC0
初期データC1
初期データCL-1
マルチプレクサ
スクランブラ
ECC部
埋め込み部
重みつきSNR計算部
セレクタ
20
22
24
26
29
30
Xb
X′b
X′c
埋め込みホストデータW

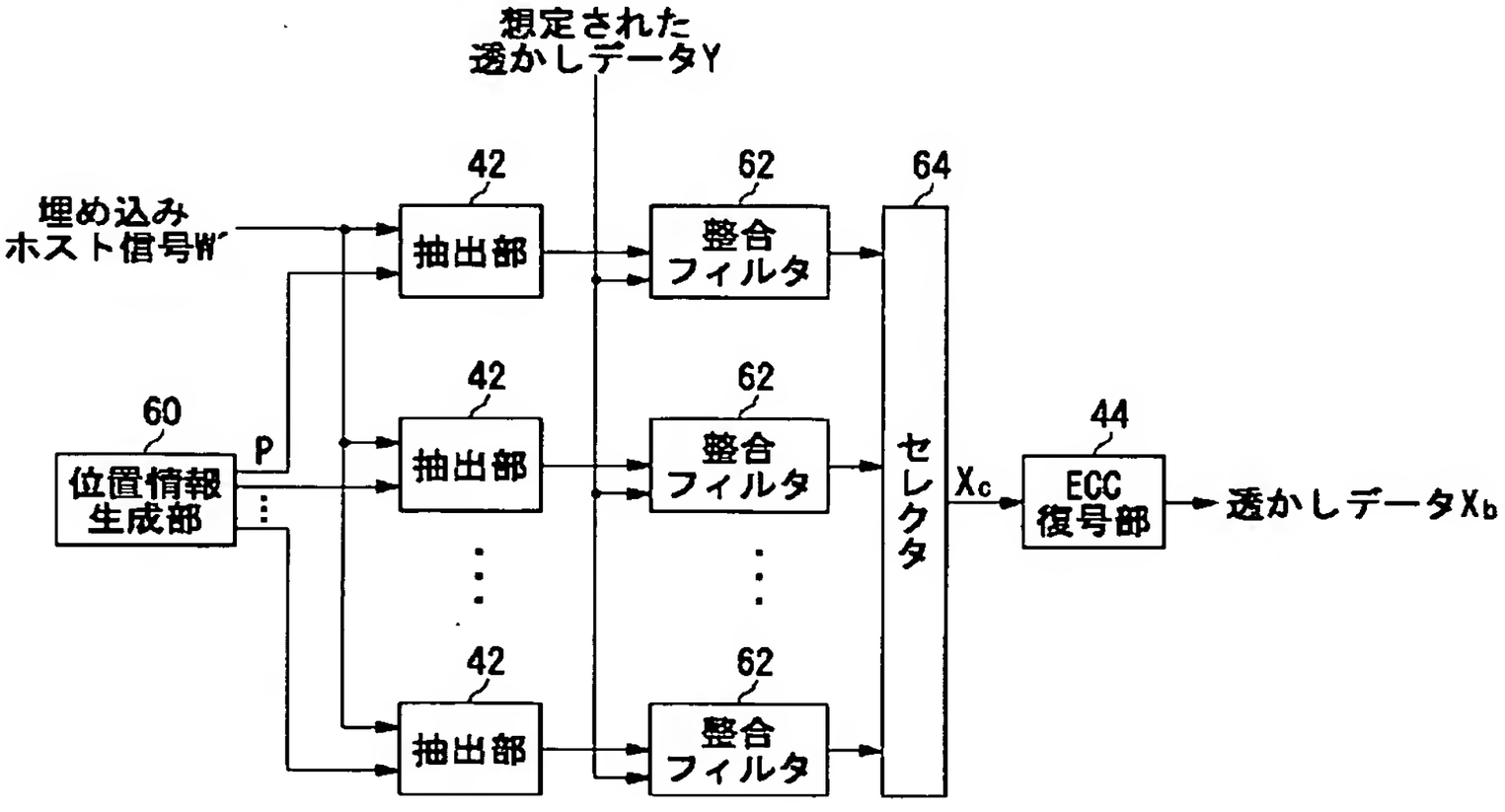
【図１２】


50
12
透かし情報I
暗号化部
X
52
位置検出部
P
54
ホストデータV
埋め込み部
埋め込み
ホストデータW
秘密鍵K

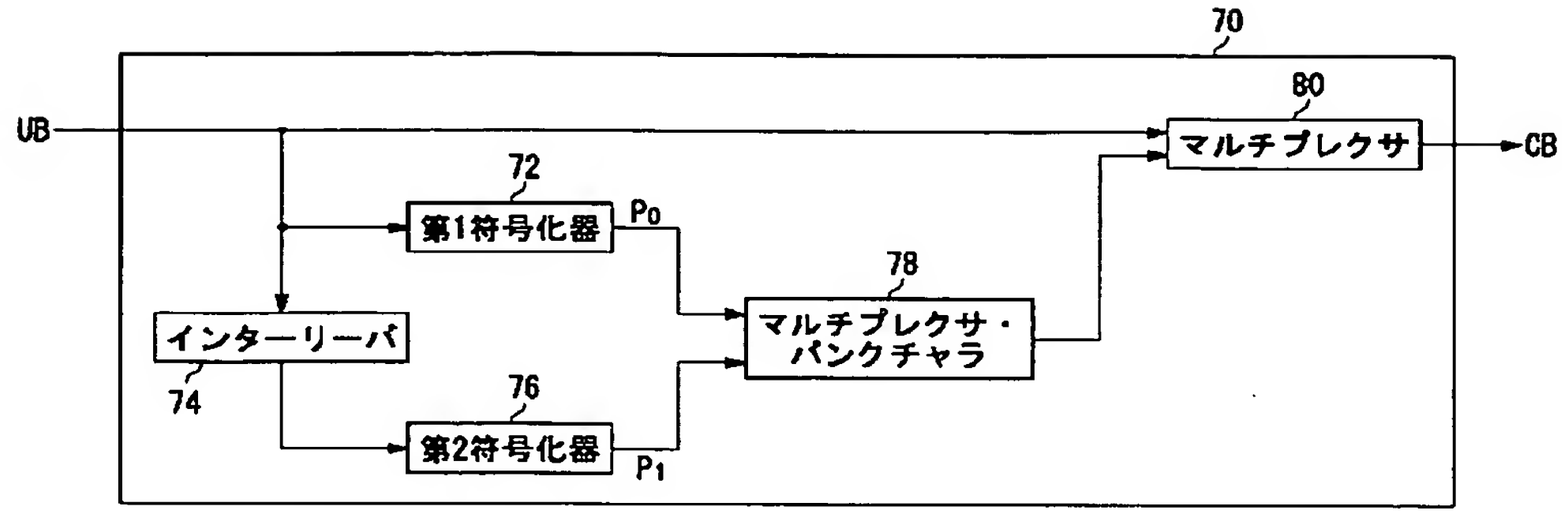
【図１３】


ホストデータV
24
26
28
30
透かしデータXb
ECC部
Xc
埋め込み部
SNR
計算部
60
位置情報
生成部
P
セレクタ
埋め込み
ホストデータW

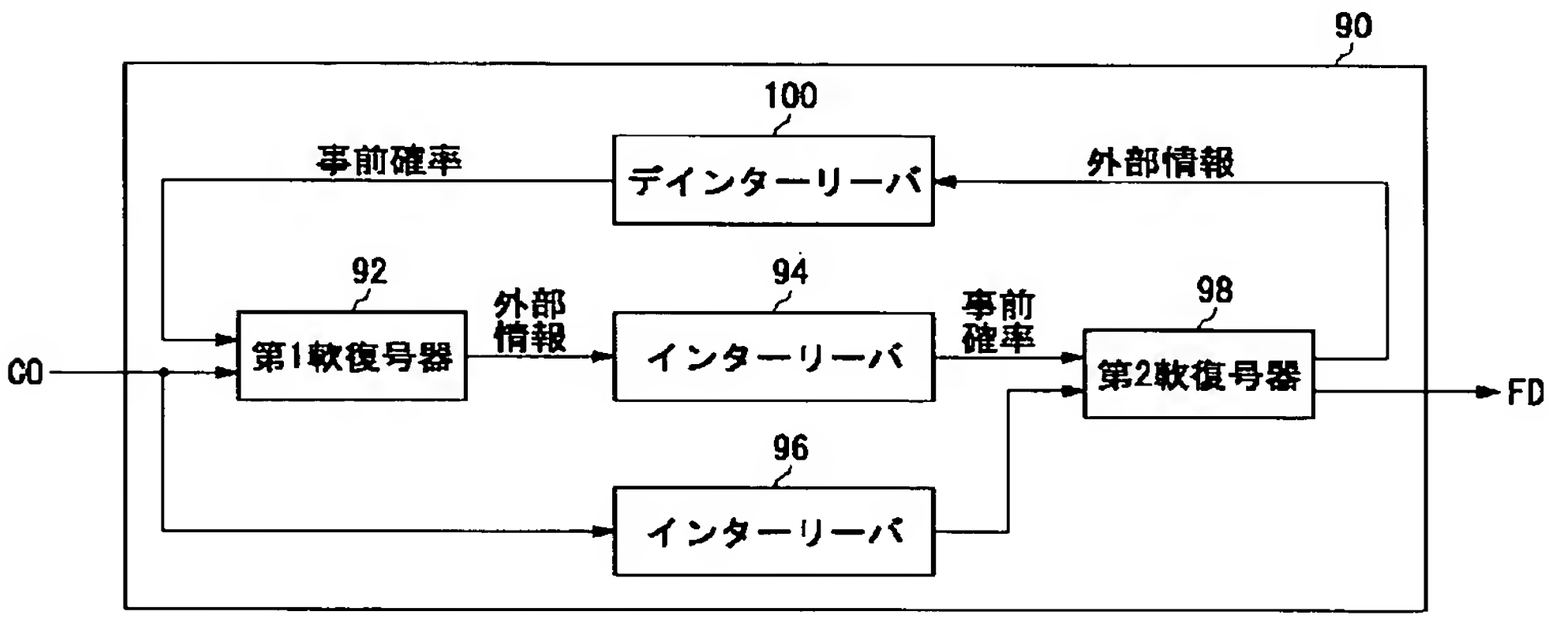
【図１４】


想定された
透かしデータY
42
62
64
埋め込み
ホスト信号W'
抽出部
整合
フィルタ
60
位置情報
生成部
P
セレクタ
44
Xc
ECC
復号部
透かしデータXb

【図１５】


70
80
UB
マルチプレクサ
CB
72
第1符号化器
P0
78
マルチプレクサ・
パンクチャラ
インターリーバ
74
76
第2符号化器
P1

【図１６】


90
100
事前確率
デインターリーバ
外部情報
92
94
98
外部
情報
事前
確率
CO
第1軟復号器
インターリーバ
第2軟復号器
FD
96
インターリーバ